

Astaro Security Linux

WebAdmin

User Manual

Astaro Security Linux V5

(Version 5.007)

User Manual

Release 3.0 – Date: 17.05.2004

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of Astaro AG.

© Astaro AG. All rights reserved.

Pfinztalstrasse 90, 76227 Karlsruhe, Germany

<http://www.astaro.com>

Portions © Kaspersky Labs.

Astaro Security Linux and WebAdmin are trademarks of Astaro AG. Linux is a trademark of Linus Torvalds. All further trademarks are the property of their respective owners.

Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to documentation@astaro.com.

Table of Contents

Contents	Page
1. Welcome to Astaro	9
2. Introduction to the Technology	10
3. Installation	18
3.1. System Requirements.....	19
3.2. Installation Instructions.....	22
3.2.1. Software Installation	22
3.2.2. Configuring the Security System.....	27
4. WebAdmin	34
4.1. Info Box.....	35
4.2. Tab List.....	35
4.3. Menus	36
4.3.1. The Status Light.....	36
4.3.2. Selection Fields.....	36
4.3.3. Drop-down Menus.....	38
4.3.4. Lists.....	39
4.4. Online Help	40
4.5. Refresh	41
5. Using the Security System	42
5.1. Basic Settings (System).....	44
5.1.1. Settings	44
5.1.2. Licensing	50
5.1.3. Up2Date Service	54
5.1.4. Backup.....	62
5.1.5. SNMP Access.....	68
5.1.6. Remote Syslog Server.....	69
5.1.7. User Authentication	71
5.1.7.1. RADIUS.....	72

Table of Contents

Contents	Page
5.1.7.2. SAM – NT/2000/XP	76
5.1.7.3. LDAP Server.....	78
5.1.8. WebAdmin Settings	91
5.1.9. WebAdmin Site Certificate	94
5.1.10. High Availability	97
5.1.11. Shut down/Restart	102
5.2. Networks and Services (Definitions)	103
5.2.1. Networks	103
5.2.2. Services	110
5.2.3. Users	114
5.3. Network Settings (Network).....	118
5.3.1. Hostname/DynDNS.....	118
5.3.2. Interfaces.....	119
5.3.2.1. Standard Ethernet Interface	124
5.3.2.2. Additional Address on Ethernet Interface	128
5.3.2.3. Wireless LAN	130
5.3.2.4. Virtual LAN	140
5.3.2.5. PPPoE-DSL Connection	145
5.3.2.6. PPTPoE/PPPoA-DSL Connections.....	150
5.3.3. Routing	155
5.3.4. NAT/Masquerading.....	157
5.3.4.1. NAT	157
5.3.4.2. Masquerading	161
5.3.4.3. Load Balancing	163
5.3.5. DHCP Server	165
5.3.6. PPTP VPN.....	169
5.3.7. Accounting.....	175
5.3.8. Ping Check.....	177

Table of Contents

Contents	Page
5.4. Intrusion Protection	179
5.4.1. Settings	179
5.4.2. Rules	182
5.4.3. Advanced	186
5.5. Packet Filter	188
5.5.1. Rules	188
5.5.2. ICMP	200
5.5.3. Advanced	203
5.6. Application Gateways (Proxies)	209
5.6.1. HTTP/Surf Protection	210
5.6.2. DNS	227
5.6.3. SOCKS	229
5.6.4. POP3	232
5.6.5. Ident	237
5.6.6. SMTP	238
5.6.6.1. Virus Protection/Content Filter	243
5.6.6.2. Spam Protection	248
5.6.7. Proxy Content Manager	255
5.7. Virtual Private Networks (IPSec VPN)	260
5.7.1. Connections	269
5.7.2. Policies	277
5.7.3. Local Keys	282
5.7.4. Remote Keys	285
5.7.5. L2TP over IPSec	288
5.7.6. CA Management	290
5.7.7. Advanced	295

Table of Contents

Contents	Page
5.8. System Management (Reporting)	298
5.8.1. Administration	298
5.8.2. Virus	299
5.8.3. Hardware.....	299
5.8.4. Network.....	300
5.8.5. Packet Filter	301
5.8.6. Content Filter.....	301
5.8.7. PPTP/IPSec VPN.....	302
5.8.8. Intrusion Protection	302
5.8.9. DNS	302
5.8.10. HTTP Proxy Usage	302
5.8.11. Executive Report	302
5.8.12. Accounting.....	303
5.8.13. System Information.....	305
5.9. Local Logs (Log Files)	307
5.9.1. Settings	307
5.9.2. Local Log File Query.....	311
5.9.3. Browse	312
5.9.3.1. Log Files	316
5.9.3.2. Error Codes.....	320
5.10. Online Help	333
5.11. Exiting the Security Solution	334
Glossary	335
Index	342

1. Welcome to Astaro

Congratulations on your purchase of the Internet Security Solution Astaro Security Linux V5, and welcome to the Astaro family.

This manual will take you step-by-step through the installation process, will explain the web-based WebAdmin™ configuration tool, and can be used to document your configuration.

The most recent version of this document is always available at the following address:

<http://docs.astaro.org>

In order to provide you with the most up-to-date information possible, this document makes occasional reference to other documents available at the web sites of Astaro and other organizations. Please note that these addresses may change over time, and that documents hosted by other organizations may even be removed entirely.

If you have further questions, or notice any mistakes in this manual, please do not hesitate to contact us at

documentation@astaro.com

For further support, please visit our user support forum at

<http://www.astaro.org>

or make use of the Astaro Support Program.

2. Introduction to the Technology

Before exploring the Astaro Security Linux Security Solution in detail, it may be helpful to take an overview of network and security technology in general. In particular, it is important to understand the serious risks that unprotected systems face as well as where and how to deploy this security system to mitigate these risks.

Networks

The Internet is already well established as a vital communications medium and a key marketplace for both traditional and new services. Since its inception, its size has multiplied, with domain name growth between 1995 and 2002 reaching almost exponential proportions.

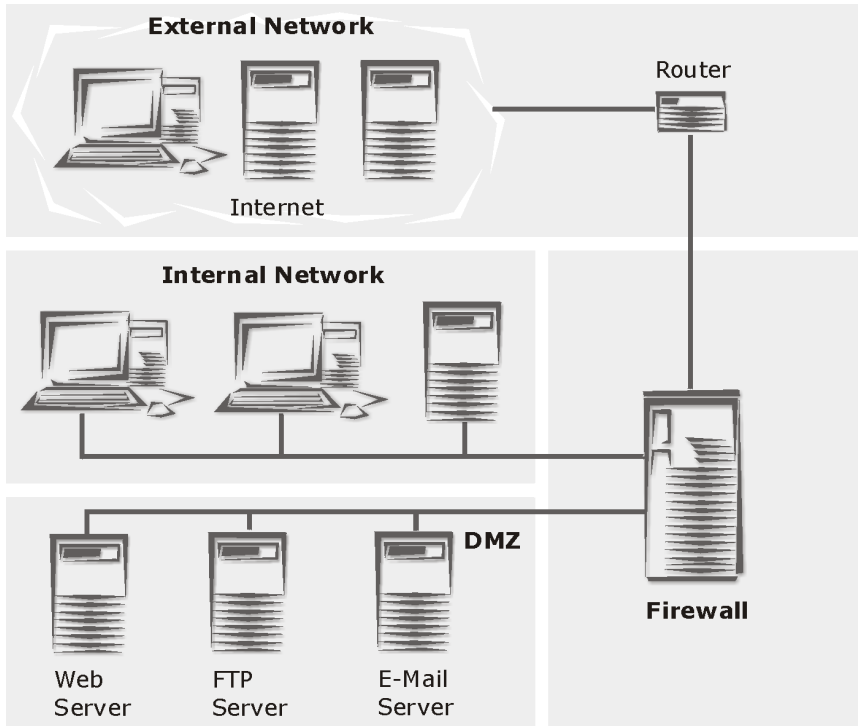
Computers on this worldwide network communicate using the **Internet Protocol (IP)**, as well as various higher-level protocols such as TCP, UDP, and ICMP. IP addresses uniquely identify each of the computers reachable on the network.

The Internet itself is a collection of smaller networks of various kinds. When two or more networks are connected, a number of issues arise which are dealt with by devices such as routers, bridges, and gateways. A firewall is another such device, designed with security in mind.

As a rule, three kinds of network meet at the firewall:

- An external or Wide Area Network (WAN)
- An internal or Local Area Network (LAN)
- A De-Militarized Zone (DMZ)

An example configuration is shown on the next page.



The Firewall

One of the components in this security system is a firewall. The characteristic tasks of a firewall connecting a WAN, LAN, and DMZ are:

- Protection against unauthorized access
- Access control
- Collection of audit trails
- Protocol analysis
- Reporting of security-related events
- Concealing internal network structure
- Separation of servers and clients using proxies

Introduction to the Technology

- Guaranteeing information confidentiality

A **firewall** combines several network components in order to provide these assurances. The following is a brief look at some of these tools and their uses.

Network-Layer Firewalls: Packet Filters

As the name suggests, this component filters IP packets on the basis of source and destination address, IP flags, and packet payload. This allows an administrator to grant or deny access to services based on factors such as:

- The source address
- The destination address
- The protocol (e.g. TCP, UDP, ICMP)
- The port number

The primary advantages of packet filters are their speed and their independence of operating systems and applications in use behind the firewall.

Advanced implementations of packet filters also inspect packets at higher network layers. Such filters interpret transport-level information (such as TCP and UDP headers) to analyze and record all current connections. This process is known as **stateful inspection**.

A stateful packet filter records the status of all connections, and allows only those packets associated with a current connection to pass. This is especially important for allowing connections from a protected network to an unprotected one, but disallowing connections in the opposite direction.

When a computer in the protected network establishes a connection with an external server, the stateful packet filter will allow the server's response packets in to the protected network. When the original connection is closed, however, the packet filter will block all

further packets from the unprotected network (unless, of course, they have been explicitly allowed).

Application-Layer Gateways: Application Proxies

The second main kind of firewall is the application-layer gateway. These gateways act as a middleman in connections between external systems and protected ones. With such gateways, packets aren't forwarded so much as translated and rewritten, with the gateway performing the translation.

The translation process on the gateway is called a **proxy server**, or **proxy** for short. Because each proxy serves only one or a few well-defined application protocols, it is able to analyze and log protocol usage at a fine-grained level, and thereby offer a wide range of monitoring and security options.

The analysis can be especially intensive at the application level, because the application data transferred conforms to standardized protocols. The firewall knows about and can inspect every aspect of the data flow. This also means that small, manageable modules can be used for each kind of data, which in turn means the system is less prone to problems due to implementation errors.

For example, this security solution includes the following proxies:

- An HTTP proxy with Java, JavaScript and ActiveX
- An SMTP proxy, which scans e-mails for viruses and controls e-mail distribution
- A SOCKS proxy which acts as a generic authenticating circuit-level proxy for many applications

Application-level gateways have the advantage of allowing the complete separation of protected and unprotected networks. They ensure that no packets are allowed to move directly from one network to the other. This results in reduced administration costs: as proxies ensure the integrity of protocol data, they can protect all of the clients

Introduction to the Technology

and servers in your network, independent of brand, version, or platform.

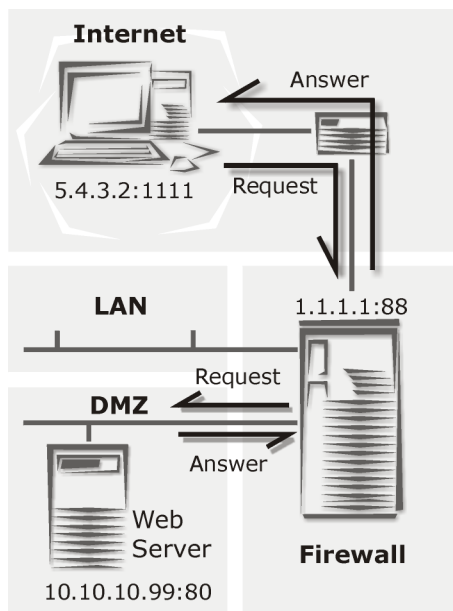
Protection Mechanisms

Some firewalls contain further mechanisms to ensure added security.

One such mechanism is supporting the use of private IP addresses in protected networks through **Network Address Translation (NAT)**, specifically

- Masquerading
- Source NAT (SNAT)
- Destination NAT (DNAT)

This allows an entire network to hide behind one or a few IP addresses, and hides the internal network topology from the outside.



This allows internal machines to access Internet servers while making it impossible to identify individual machines from the outside.

Using **Destination NAT**, it is nevertheless possible to make internal or DMZ servers available to the outside network for specific services.

Example: An external user (see graphic on left) with the IP address 5.4.3.2 sends a request from port 1111 to the web server in the DMZ. The user knows only the external IP and port (1.1.1.1, port 88).

Using **DNAT**, the firewall changes the destination address of the

Introduction to the Technology

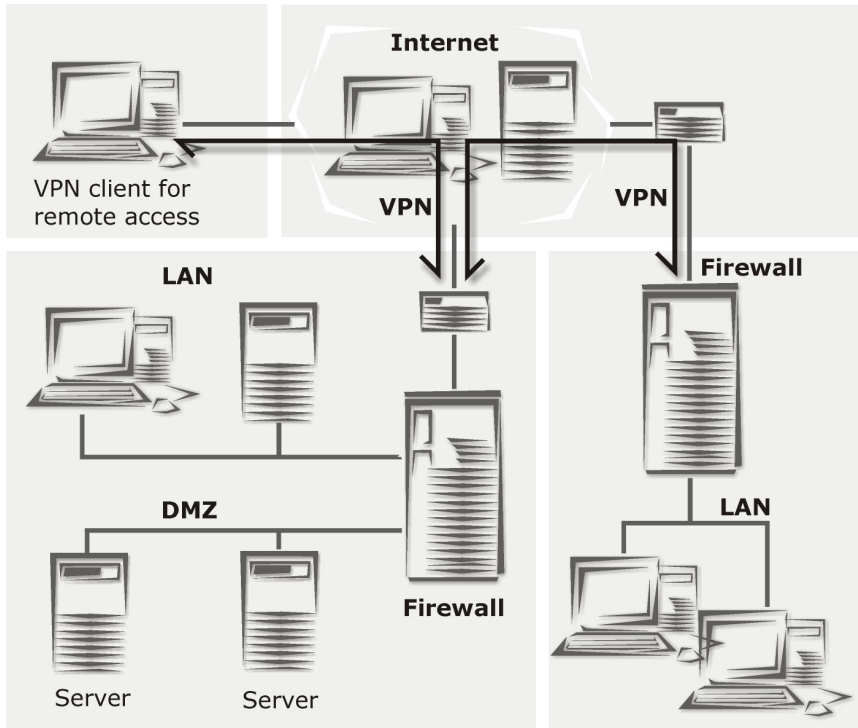
request to the internal address of the web server (10.10.10.99, port 80), and sends it to the web server. The web server then responds, using its own internal IP address (10.10.10.99), and sends the reply back to the user. The firewall recognizes the packet from the user's address and changes the source address of the reply from the web server's address to its own external address (1.1.1.1, port 88).

Another advanced protection mechanism supported by this system is VPN technology. To meet the demands of modern business, IT infrastructures must offer real-time communication and allow close cooperation between business partners, consultants, and branch offices. Increasingly, these demands are being met through the use of extranets, which usually operate either

- via dedicated lines, or
- unencrypted over the Internet.

Each of these approaches has advantages and disadvantages which must be balanced according to cost and security requirements.

Introduction to the Technology



Virtual Private Networks (VPN) provide a cost-effective solution to this problem: they can connect LANs over the Internet using encrypted connections, thus enabling secure, transparent, end-to-end communication without the need for leased lines. This is especially useful when an organization has many branch offices connected to the Internet. IPSec technology provides a standard model for these secure connections.

These secure connections can be used automatically, independent of the data being transferred – this protects the data without requiring extra configuration or passwords on the client systems.

Introduction to the Technology

ISO/OSI	TCP/IP
7 Application Layer	Application Level FTP, SMTP/E-mail
6 Presentation Layer	
5 Session Layer	
4 Transport Layer	Transmission Level TCP, UDP
3 Network Layer	Internet Level IP, ICMP
2 Data Link Layer	Network Level Ethernet
1 Physical Layer	

At the other end of the connection, the data is transparently decoded and forwarded to the recipient in its original form.

The **Firewall** component of this security system is a hybrid of the preceding protection mechanisms, combining the advantages of each:

The **Stateful Inspection Packet Filter** offers the platform-independent flexibility to define, enable, and disable all necessary services.

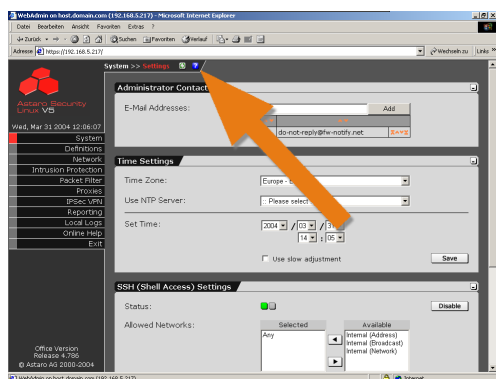
The **Proxies** incorporated into this security system transform it into an **Application Gateway** capable of securing vital services such as **HTTP**, **Mail** and **DNS**. Further, the SOCKS proxy enables generic circuit-level proxying for all proxy-aware applications.

VPN, **SNAT**, **DNAT**, **Masquerading** and **static routing** capabilities make the firewall a powerful connection and control point on your network.

Installation

3. Installation

The installation of this Internet security solution proceeds in two main steps: loading the software, and configuring the system parameters. The initial configuration required for loading the software is performed through the console-based **Installation Menu**, while the final configuration and customization can be performed from your management workstation through the web-based **WebAdmin** interface.



While configuring your system, please note that the **WebAdmin** system provides additional information and help through its **Online Help** system. To access this system, simply click the button marked ?.

The following pages contain configuration worksheets where you can enter the

data (such as default gateways and IP addresses) you use to set up your system. We recommend you fill these out as you configure the system, and that you keep the worksheets in a safe place for future reference.

Attention:

If you are upgrading your system from version 4 to version 5, and you wish to keep the settings from your existing installation, you must first upgrade your system to version 4.021 at least. Only backup files from this or higher versions of Astaro Security Linux can be loaded into Version 5. Further information on the Up2Date Service and the Backup function can be found in chapters 5.1.3 and 5.1.4.

3.1. System Requirements

The requirements for installing and using this security system are:

Hardware

- Processor: Pentium II or compatible (up to 100 users)
- Processor: Pentium III or compatible (up to 100 users)
- 256 MB RAM
- 8 GB IDE or SCSI hard drive
- Bootable IDE or SCSI CD-ROM drive
- 2 or more PCI Ethernet network cards
- For wireless LAN access: a wireless LAN PCMCIA card with the Prism2 chipset (or compatible)

Important Note:

The **High Availability (HA)**, **Wireless LAN**, and **Virtual LAN** sub-systems require extra hardware. Please check the **Hardware Compatibility List for Astaro Security Linux**, available at <http://docs.astaro.org> for compatibility.

To make Heart Beat Monitoring of the **High Availability (HA)** system easier, we recommend using network cards that support link beat for all interfaces. The installation of the **HA** system is described in detail in chapter 5.1.10 on page 97.

Installation

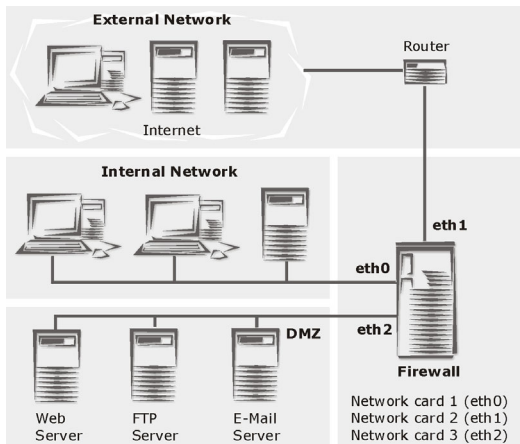
Administration PC

- Correct configuration of the **Default Gateway**, **IP Address**, and **Subnet Mask**
- An HTTPS-compliant browser (Microsoft Explorer 5.0 or newer, Netscape Communicator 6.1 or newer, or Mozilla 1.6+)

JavaScript and **Cascading Style Sheets** must be activated.

In the browser configuration, no proxies should be configured for the IP address of the eth0 interface on the firewall.

Example Configuration



As in the diagram on the left, the security system should be the only link between the internal and external networks.

Address Table

	IP Address	Network Mask	Default Gateway
Internal network interface	____.____.____.____	____.____.____.____	____.____.____.____
External network interface	____.____.____.____	____.____.____.____	
DMZ network interface ¹⁾	____.____.____.____	____.____.____.____	
Network interface for the HA system ²⁾	____.____.____.____	____.____.____.____	

¹⁾ The third and further network cards are optional.

²⁾ Network interface for the High Availability system.

Installation

3.2. Installation Instructions

What follows is a step-by-step guide to the installation process.

Attention:

The installation process will destroy all existing data on the hard disc!

Preparation

Before installation, please make sure you have the following items ready:

- The security system CD-ROM
- The Address Table, with all **IP Addresses**, **Netmasks** and **Default Gateway** filled in

3.2.1. Software Installation

The first part of the installation uses the Installation Menu to configure basic settings.

The setup program will check the hardware of the system (see screenshot), and then install the necessary software on your PC.

1. Boot your PC from the CD-ROM drive (Step 1):

In order to navigate through the menus, use the following keys. Please note the additional key functions listed in the green bar at the bottom of the screen.

Cursor keys: Use these keys to navigate through the text boxes (e.g., the license agreement or when selecting a keyboard layout)

Enter key: The entered information is confirmed, and the installation proceeds to the next step.

ESC key: Abort the installation.

Tab key: Move between text boxes, entry fields, and buttons.

Attention:

The installation will destroy all data on the PC!

2. Keyboard Layout (Step 2):

Use the **Cursor** keys to select your keyboard layout and press **Enter** to continue.

3. Hardware Test (Step 3):

The software will check the following hardware requirements: CPU, size and type of hard drive, CD-ROM drive, network cards, and IDE or SCSI controllers.

If your system does not meet the minimum requirements, the installation will report the error and abort.

4. License Agreement (Step 4):

Note:

Please read the license agreement carefully.

Press **F8** to agree to the terms of the license.

5. Time and Date (Step 5):

Use the **Cursor** keys to select your country and press **Enter** to confirm.

Use the **Cursor** keys to select your time zone and press **Enter** to continue.

Next, enter the current time and date in the entry field. Use **Tab** and the **Cursor** keys to switch between entry fields. Invalid entries will be rejected.

Confirm your entries with the **Enter** key.

Installation

6. *Network Card Selection and Configuration (Step 6):*

In order to use the **WebAdmin** tool to configure the rest of your security system, you must now configure a card to be the **internal network card (eth0)**.

Choose one of the available network cards from the list and confirm your selection with the **Enter** key.

Next, define the **IP Address**, **Network Mask**, and **Default Gateway** for this network card.

Example:

Address: 192.168.2.100

Netmask: 255.255.255.0

You must enter a value in the **Gateway** field if you wish to use the **WebAdmin** interface from a workstation outside the subnet defined by the netmask. Note that the gateway itself must be within the subnet.

For example, if you are using a netmask of 255.255.255.0, the subnet is defined by the first three values of the address: in this case, 192.168.2. If your administration computer is at, for example, 192.168.10.5, it is not on the same subnet, and thus requires a gateway to be configured here. The gateway router must have an interface on the 192.168.2 subnet, and must be able to contact the administration computer.

In our example, assume the gateway is at 192.168.2.1:

Gateway: 192.168.2.1

If the administration computer is on the same subnet as the internal network card (in our example, if its address is 192.168.2.x) it does not need a gateway. In this case, enter the following value here:

Gateway: none

Confirm your entries with the **Enter** key.

7. *Final Notes (Step 7):*

Attention:

Please read the notes and warnings presented during the installation carefully. After confirming them, all existing data on the PC will be destroyed!

If you wish to change your entries, press **F12** to return to Step 1. Otherwise, start the installation process by pressing the **Enter** key.

8. *Installing the Software (Step 8):*

The software installation process can take up to a couple of minutes. You can follow the progress of the installation using the four monitoring consoles:

There are four consoles available:

Main Installation (**Alt + F1**).

Interactive **bash** Shell 1(**Alt + F2**).

Installation Log (**Alt + F3**).

Kernel Log (**Alt + F4**).

When the installation process completes, remove the CD-ROM from the drive and connect the **eth0** network card to the internal network.

Except for the **internal Network card (eth0)**, the sequence of network cards normally will be determined by **PCI ID** and by the **Kernel** drivers.

The sequence of network card names may also change if the hardware configuration is changed, especially if network cards are removed or added.

Installation

9. Reboot the System

Reboot the security system by pressing **Ctrl + Alt + Del** or the **Reset** button.

During the boot process, the IP addresses of the internal network cards are changed. The **Install Routine** console (**Alt + F1**) may display the message `No IP on eth0` during this time.

After the security system has rebooted (a process which, depending on hardware, can take up to five minutes), **ping** the IP Address of the **eth0** interface to ensure it is reachable.

If no connection is possible, please check for the following possible problems.

Error:

The security system is not reachable from the internal network.

Possible Causes:



- The IP Address of the security system is incorrect
 - The IP Address of the client computer is incorrect
 - The Default Gateway on the client is incorrect
 - The network cable is connected to the wrong network card
 - All network cards are connected to the same hub
-

Note:

If you connect to the Internet through a **DSL** connection, please read the installation instructions at **docs.astaro.org**.

3.2.2. Configuring the Security System

The rest of the configuration will use the **WebAdmin** interface, accessed through a standard web browser (e.g., MS Internet Explorer) from your administration PC:

1. *Start your browser open WebAdmin*

Before you can access the **WebAdmin** interface, you must make sure that your browser is configured correctly. Please see in chapter 5.6.1 on page 210 for more details.

Once your browser is correctly configured, start it and enter the management address of the security system (the internal IP address configured for eth0) as follows: **https://IP Address**.

(In the example from step 6 above, this would be **https://192.168.2.100**)

A **security notice** will appear. When you generate a certificate for **WebAdmin** in a later step, this notice will disappear.

Further information on generating and installing certificates can be found in chapter 5.1.9 on page 94.

For now, simply accept the **security notice** by clicking the **Yes** button.

The first time you start **WebAdmin**, two windows will open: the first contains the **License Agreement**, and the second is used for **Setting system passwords**.

2. *Complete the License Agreement*

In the **License Agreement** window, accept the terms of the license by clicking the **I agree to the terms of the license** selection box.

Note:

Please read the terms of the license carefully.

Installation

3. Set the System Passwords

In the **Setting system passwords** window, enter the passwords for the Internet security system.



Security Note:

Use a secure password! Your name spelled backwards is, for example, not a secure password – while something like xft35\$4 would be.

You will only be able to start **WebAdmin** once you have entered passwords for the functions listed below. Enter the password for each service, and then re-enter it in the text field labeled **Confirm**. The **usernames** are pre-defined, and cannot be changed.

WebAdmin user: access to WebAdmin

This user is called **admin**.

Shell Login user: access to SSH

This user is called **loginuser**.

Shell Administrator user: administrator privileges in the entire security system.

This user is called **root**.



Security Note:

Use different passwords for the **Shell Login** and **Shell Administrator** users.

Astaro Configuration Manager User (optional): You need this password, if you wish to configure the Security system with the Astaro Configuration Manager.

Boot Manager (optional): If set, the password will prevent unauthorized users from changing boot-time parameters.

Confirm the entered passwords by clicking **Save**.

4. *Log in to WebAdmin*

User: admin

Password: Password of the WebAdmin user

Please note that passwords are case-sensitive!

Click **Login**.

Note:

Please follow steps 5 through 15 in the order listed below.

5. *Configure Basic Settings*

In the **System** tab, open the **Settings** menu and enter the following setting :

Administrator E-Mail Addresses: Enter the e-mail address of the administrator here.

You can find further information about these functions in chapter 5.1.1 on page 44.

In the **Network** tab, open the **Hostname/DynDNS** menu and enter the following settings in the **General System Settings** window:

Hostname: Enter the **Hostname** for this security system.

A domain name may contain alphanumeric characters, periods, and hyphens. The end of the name must be a valid top-level domain, such as "com", "de", or "org". The **Hostname** will be included in all **Notification E-Mails**.

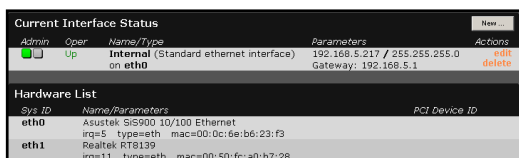
Save the settings by clicking **Save**.

Installation

6. Configure the Internal Network Interface (eth0)

In the **Network** tab, open the **Interfaces** menu and check the settings for eth0.

The settings for this network card are based on the information entered during the software installation. After starting the security system, they are shown in the **Current Interface Status** window.



Current Interface Status			
Admin	Oper	Name/Type	Parameters
Up	Up	Internal (Standard ethernet interface) on eth0	192.168.5.217 / 255.255.255.0 Gateway: 192.168.5.1

Hardware List			
Sys ID	Name/Parameters	PCI Device ID	
eth0	Asustek SiS900 10/100 Ethernet irq=5 type=eth mac=00:0c:6e:b6:23:f3		
eth1	Realtek RTL8139 irq=11 type=eth mac=00:50:fc:a0:b7:28		

If you wish to change settings for this card, for example changing the configured name, please open the **Edit**

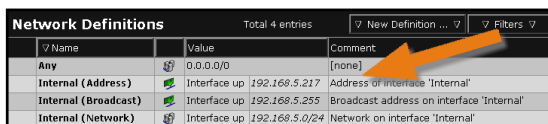
Interface window by clicking the **edit** button and make these changes now.

Attention:

If you misconfigure the **IP Address** of the **eth0** network card, you may be locked out of WebAdmin.

The configuration of network cards and virtual interfaces is described in chapter 5.3.2 on page 119.

7. Configure the Internal Network



Network Definitions			
Total 4 entries			
Name	Value	Comment	
Any	0.0.0.0/0	[none]	
Internal (Address)	Interface up 192.168.5.217	Address of interface 'Internal'	
Internal (Broadcast)	Interface up 192.168.5.255	Broadcast address on interface 'Internal'	
Internal (Network)	Interface up 192.168.5.0/24	Network on interface 'Internal'	

In the **Definitions** tab, open the **Networks** menu and check the settings

for the internal network. Three logical networks were defined during installation based on your settings for the internal network card (eth0):

The interface **Internal (Interface)**, consisting of the defined IP address (example: 192.168.2.1) and the host network mask 255.255.255.255.

The internal network **Internal (Network)**, consisting of the defined IP address (example: 192.168.2.1) and the defined network mask (example: 255.255.255.0).

The broadcast network **Internal (Broadcast)**, consisting of the broadcast address (example: 192.168.2.255) and the host network mask 255.255.255.255.

Defining new **Networks** is described in chapter 5.2.1 on page 103.

8. *Configure the External Network Card*

In the **Network** tab, open the **Interfaces** menu and configure the interface to be used to connect to the external network (Internet). The choice of interface and the required configuration depend on what kind of connection to the Internet you will be using.

The configuration of network cards and virtual interfaces is described in chapter 5.3.2 on page 119.

9. *Define Masquerading Rules*

If you wish to use private IP addresses for your internal network and wish to connect directly (without proxies) to the Internet, you can now establish the relevant rules in the **Network/NAT/Masquerading** menu.

More information about **DNAT**, **SNAT** and **Masquerading** can be found in chapter 5.3.4 on page 157.

IP routing entries for networks directly connected to the security system's network cards (**Interface Routes**) will be added automatically.

If required, you can also define routing entries manually using the **Routing** menu. This will, however, usually only be necessary in complex network environments.

Installation

10. *Configure the DNS Proxy*

In order to speed up name resolution, you can specify a local **DNS name server** (or one provided by your ISP) in the **Proxies/DNS** menu. Otherwise, the security system will automatically use the **root name servers**.

If you wish to use the proxy, you should configure the **DNS Proxy** settings now.

More information about configuring the **DNS Proxy** can be found in chapter 5.6.2 on page 227.

11. *Connect Other Networks*

If you wish to connect other internal networks to the security system, attach their cables now.

12. *Configure the HTTP Proxy*

If computers on the internal network should use the HTTP proxy to connect to the Internet, open the **HTTP** menu in the **Proxies** tab and click **Enable**.

The configuration of the **HTTP proxy** is described in more detail in chapter 5.6.1 on page 210.

Please note that the computers on the internal network will have to be configured to make use of the proxy.

13. *Configure the Packet Filter*

In the **Rules** menu under the **Packet Filter** tab, you can establish packet filtering rules.

By default, all packets are filtered until you explicitly enable certain services. New rules are added to the bottom of the list, and are inactive until explicitly enabled. The rules are processed starting with the first and moving down the list, stopping at the first applicable rule. To activate a rule, click the status light once – the status light will turn green.

Please note that, because the security system uses **Stateful**

Inspection, only the connection-building packets need be specified. All response packets will automatically be recognized and accepted.

Configuring the **Packet Filter** is described in chapter 5.5 on page 188.

14. Debug Packet Filter Rules

With the **Packet Filter Live Log** function In the **Packet Filter/Advanced** menu, you can see which packets the packet filter is filtering. If you have problems after installing your security system, this information can be helpful in **debugging** your filtering rules.

The **Packet Filter Live Log** function is described in chapter 5.5.3 on page 203.

15. Install System and Virus Scanner Updates

You should download and install the latest **System Up2Dates** as soon as possible.

If you have a license for the **Virus Protection** module, you should also run the **Pattern Up2Date** system.

The **Up2Date Service** option is described in chapter 5.1.3 on page 54.

When you've completed these steps, the initial configuration of your security system is complete. Click the **Exit** tab to leave **WebAdmin**.

Problems

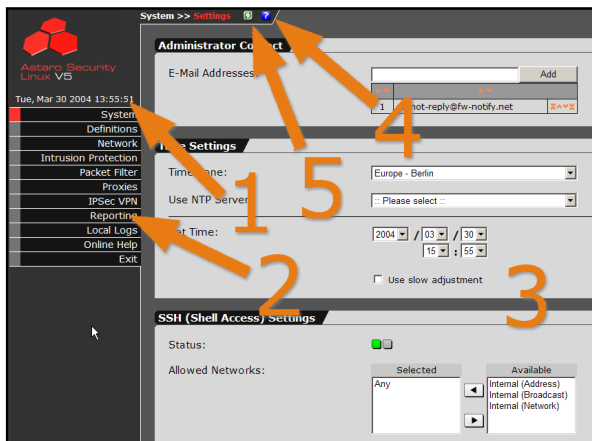
If you have problems completing these steps, please contact the support department of your security system supplier, or visit the **Astaro Bulletin Board** at:

<http://www.astaro.org>

4. WebAdmin

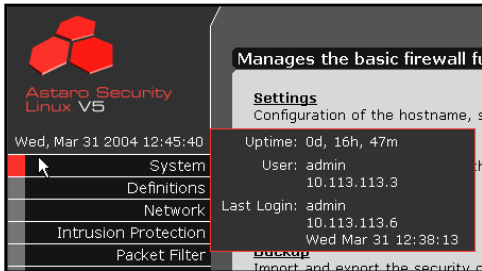
The **WebAdmin** tool allows you to configure every aspect of the Astaro Security Linux system. This chapter explains the tools and concepts used by **WebAdmin**, and shows how to use the built-in online help system.

WebAdmin has four main components:



- (1) Info Box
- (2) Tabs
- (3) Menus
- (4) Online help
- (5) Refresh

4.1. Info Box



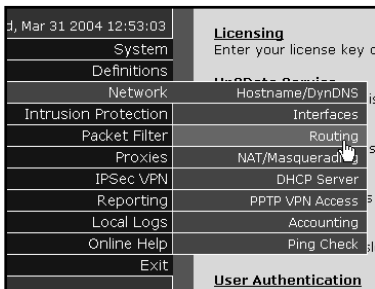
The system time and time zone are always displayed in the top left-hand corner of the screen. If you roll the mouse over the time display, the Info Box will appear, containing the following information:

Uptime: Displays how long the security system has been running without a restart.

User: Displays which user is currently logged in to **WebAdmin**, as well as the client the user is logged in from.

Last Login: Displays when and from which client **WebAdmin** was last used.

4.2. Tab List



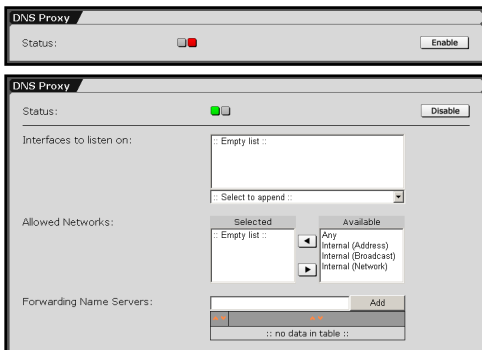
The Tab List on the left of the screen organizes the various menus according to subject. To list the menus contained under a subject heading, simply click the tab: the available menus will appear below. For ease of use, chapter 5, "Using the Security system", has been structured to match the order of topics in the Tab List.

WebAdmin

4.3. Menus

Every function of the security system has its own separate menu in **WebAdmin**. This chapter describes the tools and displays used in the configuration menus.

4.3.1. The Status Light



Many features and subsystems of the security system can be enabled or disabled while the system is running. A status light displays the current status of such subsystems:

- red = Function is disabled
- green = Function is enabled

For many features, the configuration options and tools will not be displayed until the status light is green.

4.3.2. Selection Fields

There are two kinds of selection field which are used in configuring the security system.



Selection Fields like the one at the left, called here **type A**, are used to select arbitrary groups of things like users or networks. This

kind of field is used, for example, when selecting **Allowed Networks** or **Allowed Users**.

Adding Objects to the Selected List:

1. In the **Available** list, select the object (e.g. the network or user) you wish to add by clicking its name.

You can select more than one object at a time by holding the **CTRL** key while you make your selection.

2. Click the **Left Arrow** button.

The names you selected in the **Available** window will be moved to the **Selected** window.

Removing Objects from the Selected List:

1. In the **Selected** list, choose the objects (networks or users) you wish to remove by clicking them.

Again, you can select more than one object at a time by holding the **CTRL** key while you make your selection.

2. Click the **Right Arrow** button.

The objects will be moved back to the **Available** window.



The second kind of **Selection Menu (type B)** is used to append objects to a list, for example **Authentication Methods** or **Network Interfaces**.

As a rule, the administrator must first configure these objects. If there are objects available, the drop-down list in the selection menu will display the message **Select to append**; otherwise, it will read **Empty List**.

Appending Objects to the List:

1. Open the drop-down menu.
2. Choose the object to add by clicking its name.

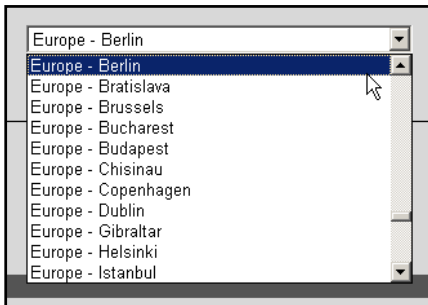
The name will be moved to the list immediately.

Removing Objects from the List:

1. Double-click the name of the object to be removed.

The object will be moved back to the drop-down menu immediately.

4.3.3. Drop-down Menus



Drop-down menus are used to configure functions that can have only one of a few values. To use, simply select the value from the list: as a rule, values chosen in drop-down menus take effect immediately.

4.3.4. Lists

		Add
Page	1 2	# 10
1	do-not-reply@fw-notify.net	⚡⚡⚡
2	mustermann@agency.com	⚡⚡⚡
3	richard.striegel@projektagentur.com	⚡⚡⚡
4	mueller@agency.com	⚡⚡⚡
5	koenig@agency.com	⚡⚡⚡
6	siegel@agency	⚡⚡⚡
7	king@agency	⚡⚡⚡
8	martin@agency	⚡⚡⚡
9	striegel@agency.com	⚡⚡⚡
10	bachmann@agency.com	⚡⚡⚡

Lists are used, in contrast, to configure functions that not only allow more than one value to be configured, and where the listed objects do not need to be first defined by the administrator. In some instances, the order of the configured values is also relevant. Each list can contain many pages of values, and each page displays ten entries.

The **Interfaces** menu, for instance, uses a list to allow access to the **Wireless LAN Access Point**.

		Add
Page	1 2	# 11
1	do-not-reply@fw-notify.net	⚡⚡⚡
2	mustermann@agency.com	⚡⚡⚡
3	richard.striegel@projektagentur.com	⚡⚡⚡

The first row of the table shows the number of pages in the list on the left (the current page is shown in white) and the total number of entries on the right (next to the # symbol). Note

that, if you roll the mouse over one of the red page numbers, a tooltip appears showing the first and last entries on that page. (See picture at right.) This can help to navigate quickly between pages.

The second row contains tools to control the display of the list. Note that these do not change the configuration information, but rather the way in which these entries are displayed within **WebAdmin**. In cases where order is important, only the order indicated by the numbers next to entries has an effect on the configuration of the function. The buttons ▲ and ▼ in the left-hand column display the list in ascending and descending numerical order respectively, while the ▲ and ▼ buttons in the middle column display the list in ascending or descending alphabetical order.

WebAdmin

The functional order, as indicated by the numbers to the left of each entry, can be adjusted using the buttons in the right-hand column. A click on the ▲ or ▼ button in this column will move the entry one row up (i.e., towards 1) or down (towards the end of the list) respectively. Similarly, you can move an entry to the very beginning or end of the list by clicking the ⚡ or ⚡ buttons in this column, respectively.

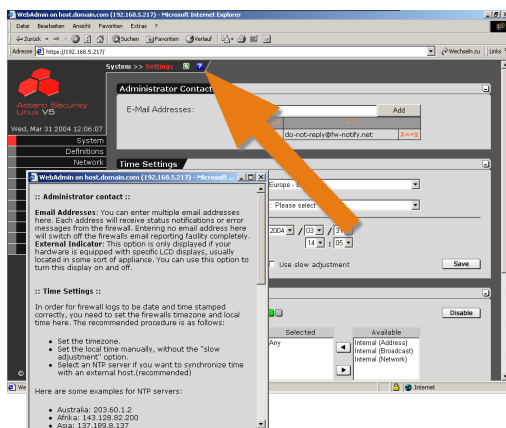
Add entry: Type a value in the text-entry field and click **Add**.

The new value will appear in the last row of the table.

Delete entry: By double-clicking an entry, you can remove it from the list.

Edit entry: If you click an entry once, it will appear in the entry field. Edit the entry as desired and click the **Replace** button to put it back into the list.

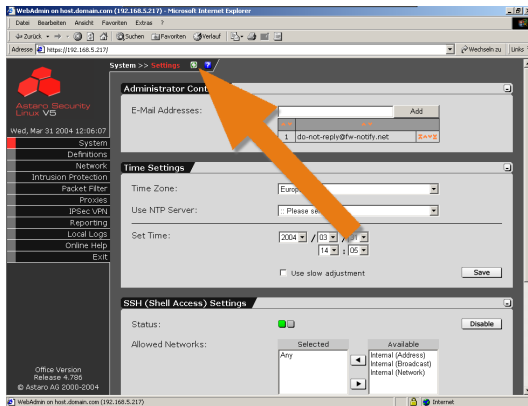
4.4. Online Help



Every menu in **WebAdmin** has an **Online Help** screen which provides a short explanation of the available configuration options.

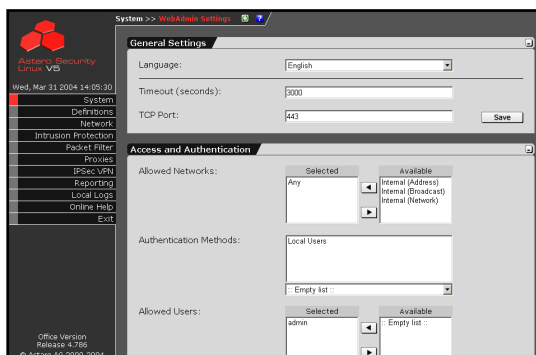
You can open the help screen by clicking the ? button at the top right-hand corner of the screen.

4.5. Refresh



To load the menu again, click the **Refresh** button. Don't use the **Refresh** button of the tool bar of your browser to actualize the menu – otherwise you are logged-off the session and have to log in again under the **WebAdmin** configuration tool!

5. Using the Security System



We have already seen the web-based configuration tool **WebAdmin** in action during the installation process. This chapter will describe how to use **WebAdmin** to control and monitor your security system on a day-to-day basis.

The specific settings, what they do, and how to change them will be described step-by-step. Please look to chapter 4 for a more general description of how to use the tools provided by the **WebAdmin** interface.

Please remember that the goal in configuring a security system like this should be to enable only the features necessary for correct functionality. In general, you should restrict in- and outbound connections to those explicitly required.

Tip:

Draw up a plan of your network and determine which computer is to have access to which **services** before configuring the security system. This will simplify the configuration process and save you a lot of time.

Configure the system as follows:

1. Define all the required networks and hosts.
2. Define the necessary services.
3. Define the system rules and proxies.

Starting WebAdmin:

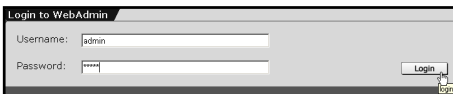
1. Start your browser and enter the address of the Security system (i.e., the address of the eth0 interface) as follows:
https://IP Address.

In our example from step 6 of the installation instructions in chapter 3.2, this would be https://192.168.2.100.

If you have not yet generated a **Certificate** for your **WebAdmin** site, a **Security notice** will appear.

More information on how to install a certificate is available in chapter on page 94.

2. Click the **Yes** button on the security notice to continue.
3. Log in to **WebAdmin**.

A screenshot of the WebAdmin login interface. It has a title bar 'Login to WebAdmin'. Below it, there are two input fields: 'Username:' with 'admin' entered, and 'Password:' with masked characters. To the right of the password field is a 'Login' button. There is also a small 'Cancel' button at the bottom right.

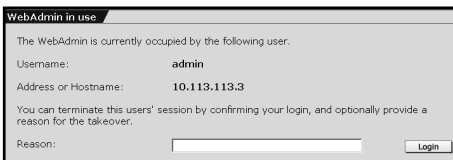
User: admin

Password: the password of the WebAdmin user.

Both entries are case-sensitive!

4. Click **Login**.

Another administrator is already logged-in:

A screenshot of a dialog box titled 'WebAdmin in use'. The text inside says: 'The WebAdmin is currently occupied by the following user.' Below this, it lists 'Username: admin' and 'Address or Hostname: 10.113.113.3'. A message follows: 'You can terminate this users' session by confirming your login, and optionally provide a reason for the takeover.' There is a 'Reason:' label followed by an empty text input field. A 'Login' button is at the bottom right.

If another administrator is already logged in to **WebAdmin**, a notice will appear on screen. The IP address shows you which

computer the other administrator is using.

The kick function allows you to end the other administrator's session.

In the **Reason** field, type a reason for ending the other user's session and click **Login**.

Using the Security System

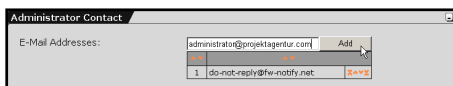
You are now logged in, and can use the **WebAdmin** to manage the system.

5.1. Basic Settings (System)

The menus under the **System** tab allow you to configure and manage the basic settings of your Security Solution.

5.1.1. Settings

Administrator Contact



E-Mail Addresses: Whenever certain important events occur, such as portscans, failed logon

attempts, or reboots, as well as whenever the self-monitor or Up2-Date systems generate alerts or reboots, the security system will send a notification e-mail to the administrator through the e-mail addresses entered into the ordered list. At least one e-mail address must be present; otherwise the **E-Mail Reporting** module will be disabled.

To add a new e-mail address, enter it in the entry field and click **Add**.

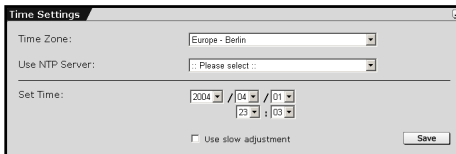
Please see chapter 4.3.4 on page 39 to learn more about the functions of the **ordered list**.

Important Note:

Notification E-Mails can only be sent to the administrator when the DNS Proxy is enabled and configured (chapter 5.6.2 on page 227), or when the **SMTP** menu (chapter 5.6.6 on page 238) has been configured with a route for incoming e-mails.

Use external Indicators: This option is only available on appliance systems with an attached LCD indicator. This option allows you to turn the LCD display on or off.

Time Settings



The screenshot shows a 'Time Settings' window. It has a 'Time Zone' dropdown menu currently showing 'Europe - Berlin'. Below it is a 'Use NTP Server' dropdown menu showing 'Please select:'. The 'Set Time' section contains four spin boxes for year (2004), month (04), day (23), and hour (03), followed by a colon and two more spin boxes for minutes (00) and seconds (00). At the bottom left is a checkbox labeled 'Use slow adjustment' which is unchecked. At the bottom right is a 'Save' button.

This menu can be used to set the time and date of the security system. The date and time can be set manually with the help of the drop-down menu or can be automatically synchronized using the NTP-server (Network Time Protocol). Please note that important changes in the time setting will appear as gaps in the **Reporting** and **Logging**.

Important Note:

We do not recommend changing the system time for daylight savings time. Instead, we recommend setting the system clock to Central European Time (CET). In summer, this corresponds to a deviation of less than one hour.

When system time settings are changed, the following "time warp" effects may be noticeable:

Moving forward (e.g., standard time to daylight saving time)

- The timeout for **WebAdmin** will expire and your session will no longer be valid.

Time-based reports will have no data for the skipped hour. In most graphs, this time period will appear as a straight line in the amount of the old value.

- **Accounting** reports will contain values of 0 for all variables during this time.

Moving backward (e.g., daylight saving time to standard time)

- There are already log data for the corresponding span of time in the time-based reports that for system purposes come from the future: These data will not be overwritten.
- Log data will be written as normal when the time point before the reset is reached again.

Using the Security System

- Most diagrams will display the values recorded during this period as compressed.
- **Accounting** reports will retain the values recorded from the “future”. Once the time point of the reset is re-reached, the accounting files will be written again as normal.

Because of these difficulties, we recommend that the time be set only during the first configuration, and that only minor adjustments be made later. We recommend setting the system clock to Central European Time (CET). This is the original time. The system then runs always in CET, not in CEST (Central European Summer Time). We recommend, not to change the time for summer, especially not when the collected reporting and accounting data are treated.

Manual configuration of system time:

1. Open the **Settings** menu in the **System** tab.
2. In the **Time Settings** window make the following settings in the given order:

Use NTP Server: In order to configure the system clock manually, please ensure that No NTP Server is selected here. In this case, the **Please select** drop-down menu will be displayed. If a NTP Server is selected, select **No NTP Server** from the drop-down menu.

Time Zone: Now select the time zone.

Note:

Changing the timezone will only change the current system time if you are using an NTP server to control time settings.

Use slow adjustment: When this function is selected, the security system will attempt to minimize the “time warp” effects mentioned above.

Note:

When resetting, the system time will be adjusted to the newly set time in small steps. When the time differences are large, this adjustment process can last days or even weeks.

Set Time: Enter the current date and time here.

Important Note:

Take note of the issue date of your License Key. If this date is after the current date set on the security system, the license will be deactivated.

The 30-day Evaluation License will not automatically activate.

5. Click the **Save** button to save these settings.

The time settings of the security system will now be updated.

Synchronizing system time with NTP Server

Before the system clock of the Internet security system can be synchronized with an external server, this server must be defined as **NTP Server**. The **NTP Server** will be defined as a network consisting of only one computer.

The definition of networks is covered in greater detail in chapter 5.2 on page 103. If the NTP server has already been defined, please begin with step 6.

1. Open the **Networks** menu in the **Definitions** tab.
2. In the **Name** entry field enter a distinct **Name**.
Allowed characters are: Letters of the alphabet, digits from 0 to 9, hyphen, space, and underscore characters. The name must be fewer than 39 characters long.
3. Now enter the **IP Address** of the **NTP Server**.

Using the Security System

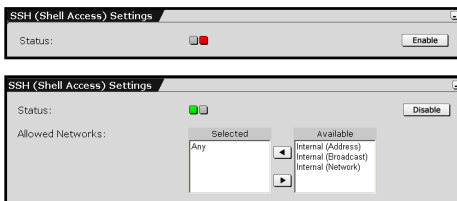
4. In the **Subnet Mask** entry field, enter the **network mask** 255.255.255.255.
5. Now confirm your settings by clicking on the **Add** button.
WebAdmin will now check your entries for semantic validity. Once accepted, the new network will appear in the network table.
6. Open the **Settings** menu in the **System** tab.
7. In the **Time Settings** window make the following settings in the given order:

Time Zone: Now select the time zone.

Use NTP Server: Select the NTP Server here.

The system clock of the Internet Security system will be synchronized with the external NTP server every hour.

SSH (Shell Access) Settings



Secure Shell (SSH) is a text-based access mode for the security system intended only for advanced administrators. In order to access this shell, you will need an **SSH Client**, which

comes standard with most Linux distributions. For MS-Windows, we recommend **PuTTY** as SSH Client. Access through **SSH** is encrypted, and cannot be read by eavesdroppers.

The Shell Access function is enabled by default, once you have entered a password for the configuration through the **Astaro Configuration Manager** in the **Setting System Passwords** window.

If you wish to access the security system through **SSH**, the SSH Status light must be enabled (status light shows green).

The **SSH** protocol uses **name resolution** (valid name server) if no valid name servers are found, SSH access attempts will time out. The time-out takes about a minute. During which time the connection seems to be frozen or failed. Once the time-out has expired, the connection process continues without further delay.

You must also add the networks allowed to access the **SSH** service in the **Allowed Networks** selection field. In order to ensure a seamless installation process, the **Allowed networks** field contains the **Any** option by default, this means that any computer can access the SSH service. Networks can be defined in the **Definitions/Networks** menu.

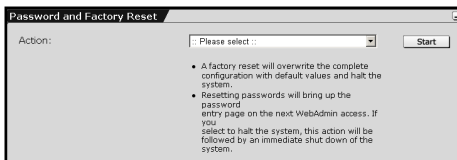


Security Note:

By default, anyone has access to the SSH service. The **Allowed Networks** field contains the **Any** option. For increased security, we recommend that access to the SSH service be limited. All other networks should be removed!

We recommend that the **SSH** service be disabled when not in active use.

Password and Factory Reset



The **Password Reset** function allows you to set new passwords for the Security system. If you log in to the **WebAdmin** configuration tool for the first

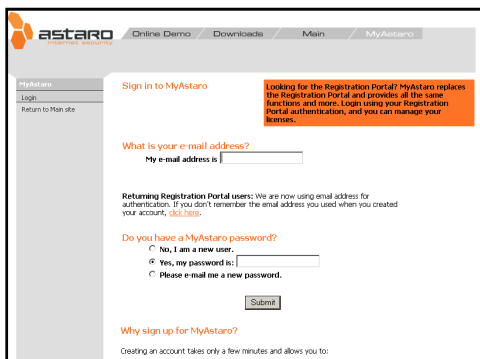
time after this action, the **Setting System Passwords** window will be displayed. This allows you to set optional passwords, such as the Astaro Configuration Manager Password. **Halt System** will shut down the Security system. After the restart, the **Setting System Passwords** window will be displayed at first.

Using the Security System

The **Factory Reset** function resets all configuration settings and options to their original state. All data entered after the initial installation will be deleted, including the **HTTP Proxy Cache**, the entire **E-Mail Queue**, **Accounting** and **Reporting** data, passwords, and uninstalled **Up2Dates**.

The software version will not change. That is, all **System Up2Dates** and **Pattern Up2Dates** that have been installed will be retained.

5.1.2. Licensing



Some of the functions of the security system, including the **Up2Date Service**, **High Availability (HA)**, **Surf Protection**, **Virus Protection** and the **Support** service from the Astaro partners, can only be used with a valid **License Key**. You can obtain detailed information about licensing and the corres-

ponding licence keys at any certified Astaro Partner, or from Astaro: **salesus@astaro.com** (America's) and **sales@astaro.com** (Europe, Asia Pacific and Africa).

First you need the **Activation Key**. With this *Activation Key* you enable the *License Key* in **MyAstaro**. This allows you to select the licensing period of the Internet security system yourself. You can thus first install the software and then register your licence in the licence portal - only from this moment of time on, starts the time period for the acquired options.



Note:

The **Activation Keys** cannot be used directly in the **WebAdmin** configuration tool. Please register at **MyAstaro** first.

Creating an User Account:

1. Open your browser and go to the site <https://my.astaro.com>.
2. Log in under **MyAstaro**.

What is your e-mail address?

The e-mail address is used for the authentication. As new customer enter the e-mail address into this entry field.

If you have already used the **Registration Portal** for **Astaro Security Linux V4**, enter the e-mail address that you have used for this registration into the entry field. If you don't remember the e-mail address that you used, you can request it under the **Returning Registration Portal users** dialogue. You'll need your **Username** and the **Password**.

Do you have a MyAstaro password?

If you log in for the first time under *MyAstaro*, click on the **No, I am a new user** check box. If you are already a user of MyAstaro, enter the password into the **Yes, my password is** entry field.

Then click on the **Submit** button.

3. Create a new **MyAstaro Account**.

E-Mail Address: You can correct your address in this entry field.

Password: Enter your desired password here.

First Name: Enter your first name here.

Last Name: Enter your last name here.

Then click on the **Register** button.

Using the Security System

If the registration was successful, the page with the message **Congratulations, you have created your MyAstaro account** will be displayed. Moreover, you receive a confirmation by e-mail.

Now you can download different versions of the Internet security system under **MyAstaro** and execute the following actions for your license:

1. Convert a Version 4 license to a Version 5 license
2. Register purchased Version 5 Activation Keys
3. Add options to your registered license
4. Download a free Home User license
5. Download a 30 days test version with additional features

Licensing the Internet security system:

In order to license the Internet security system, you need a valid license file on the local host, so that you can import it to the Internet security system through the **WebAdmin** configuration tool.

1. Open the **Licensing** menu in the **System** tab.
2. In the **Upload License File** entry field, click on the **Browse** button.
3. From the **Select File** dialogue, select the license file and click on the **Open** button.
4. Click on the **Start** button.

The system will require between 30 and 60 seconds to generate the system. After successful registration, the **License Information** window will contain the details of your license.

Licensing Information

After successful registration of the Internet security system, the License Information window will show the details of your license.

Licensed Users (IPs)

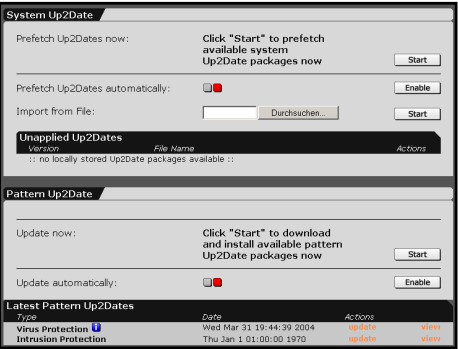
The functions in this window are used for licenses that do not allow for an unlimited number of users (IP-addresses).

View current User (IP) Listing: Clicking on the **Show** button opens a table that lists all current users through their respective IP-address.

Reset User (IPs) Listing: If you wish to reconfigure the internal network, you can reset the user table by this action. Then there is a reboot - the system will shut down completely and reboot. This action is enabled by clicking on the **Start** button.

Using the Security System

5.1.3. Up2Date Service



The **Up2Date Service** makes it easy to keep your security system software updated: New virus definitions, system patches, and security features will be installed to your current system.

All **Up2Date** data are digitally signed and encrypted, and are transferred over a secure chan-

nel. Only Astaro is entitled to create and digitally sign new **Up2Dates** packages. Any unsigned or forged **Up2Date** packages are rejected and deleted.

Astaro maintains a number of servers for both **System Up2Date** and **Pattern Up2Date** that are dialed in the given sequence. If the first Up2Date server is not available, the system will automatically query the next system or pattern Up2Dates in the list.

Important Note:

In order to download updates, the **Up2Date Service** makes a TCP connection to the update server on port 443. The security system will permit this connection without any adjustment. If there is another security system in place upstream, you must allow the communication via the port 443 TCP to the update servers.

Note:

When using the **High Availability (HA)** system, please note the special functions of **System Up2Date**.

System Up2Date

The **System Up2Date** function allows you to import system patches and new security features into your Internet security system. The **Up2Date** packages can be downloaded either manually over an encrypted connection or automatically from the Update Server. If you don't have an Internet connection, you can also import Up2Date packages from a local volume.

Newly imported Up2Date packages are presented with their respective version number and file name in the **Unapplied Up2Dates** table. These Up2Date packages have not been installed yet!

In order to get further information, touch the **blue info button** with the cursor. If the info button is highlighted **red**, there will be an automatic **restart** of the Security system after the installation of the System Up2Date package.

Note:

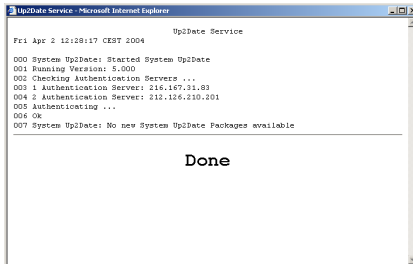
If you are using the **High Availability (HA)** system, please note the special notes for the import and installation of the **System Up2-Dates**. The **HA** system is described in chapter 5.1.10 on page 97.

Individual Up2Date packages can be downloaded from **<http://download.astaro.com/ASL/up2date>** and saved on your local computer.

Using the Security System

Manually downloading System Up2Dates:

1. Open the **Up2Date Service** menu in the **System** tab.
2. In the **System Up2Date** window, click the **Start** button under **Prefetch Up2Dates now.**



The system will now check if there are any new updates on the Update server, and will download any updates found. Details on the Up2-Date process can be found in the **Log Window**, shown in real-time (left-hand picture). When the **DONE** message appears, the process has completed successfully.

The **Unapplied Up2Dates** table lists any updates that have been downloaded but not yet installed!

If you are using the **HA** system, unapplied updates will be listed in the **Unapplied Up2Dates Master** window.

Automatic download of System Up2Dates:

1. Open the **Up2Date Service** menu in the **System** tab.
2. Click the **Enable** button under **Prefetch Up2Dates automatically.**
3. In the selection menu **Interval**, specify how often the security system should contact the **Up2Date Server** to check for new **System Up2Dates.**

The available choices are: every hour, every day, or once per week.

Newly imported Up2Date packages are presented with their respective version number and file name in the **Unapplied Up2Dates** table. Further information is available by clicking the Info button.

Note that the Unapplied Up2Dates in the table have not yet been installed yet!

If you are using the **HA** system, unapplied updates will be listed in the **Unapplied Up2Dates Master** window.

Loading System Up2Dates from a local disk:

The filename of an Up2Date update consists of the version number, **tar** to signify it is an encrypted archive file, and the file extension **.gpg**. Example: 3.033.tar.gpg. Up2Date packages can be downloaded from the **ftp.astaro.com** FTP server.

1. Open the **Up2Date Service** menu in the **System** tab.
2. In the **System Up2Date** window, click on the **Browse** button next to **Import from File**.
3. In the **File Upload** window, choose the Up2Date packages you would like to load and click on the **Open** button.

Important Note:

When using Microsoft Windows, make sure not to use a **UNC Path**. Instead, choose the updates by using the **Look in** option.

-
4. In the **System Up2Date** window, next to **Import from File**, click **Start**.

Successfully loaded updates will appear in the **Unapplied Up2Dates** window with the version number and the file name. Further information is available by clicking the Info button.

Note that the Unapplied Up2Dates in the table have not yet been installed yet!

Using the Security System

If you are using the **HA** system, unapplied updates will be listed in the **Unapplied Up2Dates Master** window.

5. Repeat steps 2 through 4 until all Up2Date packages have been imported.

Installing System Up2Dates without the HA Solution:

1. Open the **Up2Date Service** menu in the **System** tab.
2. In the **Unapplied Up2Dates** table, choose the Up2Date updates to install.

Note:

If more than one **System Up2Date** file is listed in the table, start the **highest** version. The smaller versions will be installed automatically.

3. In the **Actions** column, click **Install**.

The progress of the Up2Date installation on system 1 will be displayed in real time in the **Log Window**. When the **DONE** message appears, the process has completed successfully.

Installing System Up2Date with the HA solution:

1. Open the **Up2Date Service** menu in the **System** tab.
2. In the **Unapplied Up2Dates Master** table, choose the Up2Date updates to install.

Note:

If more than one **System Up2Date** file is listed, start with the **smallest** version. Only one package can be installed with the **HA** system.

4. In the **Actions** column, click **Install**.

Using the Security System

The progress of the Up2Date installation on system 1 will be displayed in real time in the **Log Window**. When the **DONE** message appears, the process has completed successfully.

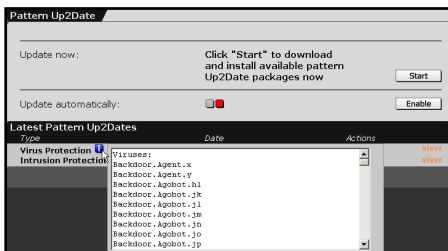
Then the installation automatically starts on system 2. During this process, the Up2Date package and the message **Polled by slave** will be displayed in the **Unapplied Up2Dates Slave** table.

The table will show the message **No locally stored Up2Date packages available** when the installation on system 2 has completed successfully.

5. If the **Unapplied Up2Dates Master** table lists more unapplied updates, repeat steps 2 and 3 until all updates have been installed.

The **HA** system is fully updated when the **Unapplied Up2Dates Master** table shows the message **No locally stored Up2Date packages available** and if both systems display the same version number.

Pattern Up2Date



The **Pattern Up2Date** function updates the virus patterns for the security system's integrated virus scanner and the Intrusion Protection System (IPS) with IPS attack signatures. You can choose to update signatures manually or automatically at certain intervals.

The **Latest Pattern Up2Dates** table shows the date of the most recently installed **Pattern Up2Date**. Virus Protection Patterns and Intrusion Protection attack signatures will be listed separately.

Using the Security System

Manual Pattern Up2Date:

1. Open the **Up2Date Service** menu in the **System** tab.
2. In the **Pattern Up2Date** window, click the **Start** button under **Update now**.

The system checks now, whether new Pattern Up2Date packages are available on the Update Server, downloads and installs them to the Internet security system. Details on the complete Up2Date process can be found in the **Log Window**, shown in real-time. When the **DONE** message appears, the process has completed successfully.

The **Installed Pattern Date** will be updated when you click the **Up2Date Service** under the **System** tab, or when you next open this menu.

When using the **High Availability (HA)** solution, the virus scanner on system 2 will be automatically synchronized with system 1.

Automatic Pattern Up2Date:

1. Open the **Up2Date Service** menu in the **System** tab.
2. Click the **Enable** button under **Update automatically**.
3. In the selection menu **Interval**, specify how often the security system should contact the **Up2Date Server** to check for new **Pattern Up2Dates**.

The available choices are: every hour, every day, or once per week.



Security Note:

Choose the hourly update option to ensure that your system is always up to date.

Using the Security System

The automatic **Pattern Up2Date** is now activated. The Security system will contact the **Up2Date Server** at regular intervals and check for new **Pattern Up2Dates**. Whenever new **Pattern Up2Dates** are installed, the administrator will be sent an e-mail containing a list of the newest virus signatures.

When using the **High Availability (HA)** solution, the virus scanner on system 2 will be automatically synchronized with system 1.

Using the Security System

5.1.4. Backup

The screenshot shows the 'Backup' configuration window with three tabs: 'Restore a Backup', 'Create a Backup', and 'Advanced'. The 'Restore a Backup' tab is active, showing an 'Upload Backup File:' field with a 'Durchsuchen...' button and a 'Start' button. The 'Create a Backup' tab is also visible, showing a 'Comment:' field and a 'Start' button. The 'Advanced' tab is partially visible, showing settings for 'Encryption' (checked), 'Passphrase' (empty field), 'Confirmation' (empty field), 'Send Backups by E-Mail' (checked), 'E-Mail Addresses' (empty table with an 'Add' button), and 'Interval' (set to 'Every day').

The **Backup** function allows you to save the settings of your Security system to a file on a local disk.

This backup file allows you to install a known-good configuration on a new or misconfigured security system. This is especially useful in case of hardware failure, as it means replacement systems can be up and running within minutes.

Attention:

Version 5.0 of the security system can only load backups from version 4.021 or higher.

Install the License Key in the **Licensing** menu before loading the backup. Without the appropriate license, the system will only support three network cards – under certain circumstances, this can lead to **WebAdmin** not being reachable.

Note:

After every system change, be sure to make a backup. This will ensure that the most current security system settings are always available. Make sure that backups are kept securely, as the backup contains all of the configuration options, including certificates and keys.

After generating a backup file, you should always check it for readability. It is also a good idea to use an external MD5 program to generate checksums: this will allow you to check the integrity of the backup later.

Restore a Backup

This window allows you to install the backup file of the configuration.

Loading a Backup:

1. Open the **Backup** menu in the **System** tab.
 2. In the **Restore a Backup** window next to the **Upload Backup File** entry field, click on the **Browse** button.
 3. In the **File Upload** window, choose the Backup file, you would like to load and click on the **Open** button.
-

Note:

When using Microsoft Windows, make sure not to use a **UNC Path** for loading the backup. Select the Backup file with the help of the **Look in** selection window.

4. Click on the **Start** button.

If, during the generation of the backup file, the **Encryption** function was enabled, the **Enter Passphrase** window will open.

5. In the **Passphrase** field, enter the password.

Using the Security System

6. Confirm your settings by clicking **Start**.

The security system will now load and check the backup file. If the checksums are correct, you will now receive the **Backup Information**.

7. Check the **Backup Information**.
8. To import the backed-up settings into the active system, click the **Start** button.

When the message **Backup has been restored successfully** appears, the process has completed successfully.

Create a Backup

This window allows you to create and archive a backup file of the configuration of your Security system.

Manually Creating a Backup:

1. Open the **Backup** menu in the **System** tab.
2. In the **Create a Backup** window, in the **Comment** field, enter a description of this backup.
When restoring system backups, this description will be displayed to help distinguish between different configurations.

Important Note:

If the **Encryption** function has been enabled, the backup file will be encrypted with either the **DES** or **3DES** algorithms, and can only be read or loaded using the correct password.

3. To generate the backup file, click the **Start** button.
The system will now generate a backup file. When the message **Backup has been restored successfully** appears, the process has completed successfully.
4. To copy the backup file to your local PC, click the **Save** button.

Using the Security System

5. On the **File download** menu, choose the **Save file to disk** and click the **OK** button.
6. Choose a descriptive file name on the **Save file as** menu.
The security system will automatically produce file names, consisting of backup, date and time:
backup_yyyymmdd_hhmmss.abf (astaro-backup-file).
7. Check the generated backup file for readability by importing it back into WebAdmin and clicking on the **Start** button.

The security system will now load and check the backup file. If the ckecksums are correct, you will now receive the **Backup Information**.
8. Abort the restore process by opening a different menu within the tab.

Attention:

After each system change, create a new backup file. If you load a new backup file and if, for example, you have changed the IP address or forgotten the password, you might not be able to access the newly configured system.

Using the Security System

Advanced

Encryption: The backup file contains all configuration settings as well as the respective certificates and keys. The **Encryption** function allows you, to encrypt the file using **DES** or **3DES**.

Encryption of e-mail Backup Files:

1. Open the **Backup** menu in the **System** tab.
2. Scroll to the **Advanced** window.
3. Enable the **Encryption** function by clicking on the **Enable** button.

The **Encryption** function is enabled, when the status light shows green.

4. In the **Passphrase** entry field, enter the password.
-



Security Note:

With passwords with up to seven characters, the Backup file will be encrypted with **DES** and from eight characters on with **3DES**.

5. To confirm, enter the password again into the **Confirmation** entry field.
6. Click the **Save** button to save these settings.

All Backup files that have been created manually or automatically by the system, will now be encrypted with the defined password.

Important Note:

A backup file that has been encrypted with **Encryption** can only be loaded to the system with the password that was used for the creation of the Backup.

Send Backups by E-Mail: The Security system can also send you automatically created backup files by e-mail, so that you don't have to remember to save the settings of your Internet security system manually on a data carrier. Then the file is e-mailed to the entered e-mail address. These e-mailed files are about 100 kilobytes long.

Generating an E-Mail Backup File:

1. Open the **Backup** menu in the **System** tab.
2. In the **Advanced** window enable the **Send Backups by E-Mail** function by clicking on the **Enable** button.

The **Backups by E-Mails** function is enabled, if the status light shows green.

Important Note:

If the **Encryption** function has been enabled, the backup file will be encrypted with either the **DES** or **3DES** algorithms, and can only be read or loaded using the correct password.

3. Use the **Interval** drop-down menu to define how often backups should be made.

The available choices are: Daily, weekly, and monthly.

4. In the **E-Mail to** field, enter the e-mail addresses, which should receive the backup files in regular intervals.
5. Click the **Add** button next to the **E-Mail to** entry field, to add this address to the ordered list.

If you would like to add more addresses, repeat step 5.

6. If you wish to generate and send a backup file immediately, click the **Start** button next to **Send backup now**.
7. Check the generated files for readability by importing the respective backup file and clicking on the **Start** button.

Using the Security System

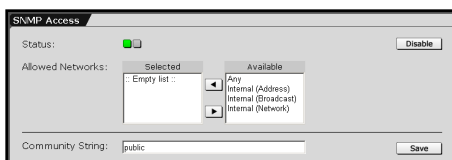
The security system will now load and check the backup file. If the checksums are correct, you will now receive the **Backup Information**.

8. Abort the restore process by opening a different menu within the tab.

Editing E-Mail Addresses:

Please see chapter 4.3.4 on page 39 for a description of how to use the **ordered list**.

5.1.5. SNMP Access



The **Simple Network Management Protocol (SNMP)** monitors and manages the local network. *SNMP* allows the administrator to make quick queries

about the condition of the network devices, such as the number and configuration of the network interfaces, the forwarded traffic, the current processes and hard disk utilization. Next to the current state, tendencies and time rows are interesting. They give a detailed insight into the functions of a network – the history can be monitored and remedied before turning into a real problem.

Configure the access rights to the *SNMP* service in the **SNMP Access** window. The users of the configured networks can then conduct queries about the *SNMP* server on the Security system with their read only rights.

Security Note:

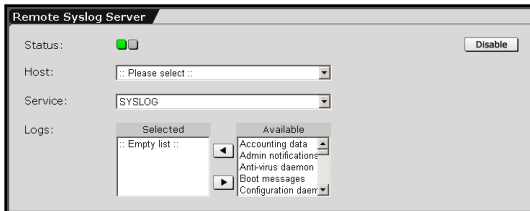


The **SNMP** data traffic (Protocol version 2) between the Security system and the network is not encrypted.

Authorizing access to the SNMP server:

1. Enable **SNMP Access** by clicking the **Enable** button.
2. From the **Allowed Networks** selection field, select the networks that you wish to allow for accessing the *SNMP* server.
3. Enter the **Community String** in this entry window.
4. Save your configuration by clicking **Save**.

5.1.6. Remote Syslog Server



This function allows you to forward log messages from the Security system to other hosts. This is especially useful for networks using a log host to collect logging information

from a number of different hosts. By default, this function is disabled. A *Logging Daemon*, compatible with *Syslog* protocol must be running on the selected host.

Attention:

In the **System/Remote Syslog Server** menu, do not select one of the security system's interfaces (such as eth0) as the destination address (host).

Host: Enter the host, which should receive logging information in the drop-down menu. When a host has been selected, log forwarding is enabled immediately: no further messages are displayed.

In order to select a logging host (i.e., a network with netmask 255.255.255.255) you will first have to define it in the **Definitions/Networks** menu. The definition of networks is covered in greater detail in chapter 5.2 on page 103.

Using the Security System

Service: The **Syslog** protocol is set by default. You can also use this drop-down menu to configure the service (port) that should be used on the remote server.

Logs: This selection field allows you to select log files that should be delivered to the Remote Host.

5.1.7. User Authentication

The security system supports **User Authentication** using the SOCKSv5, SMTP, and HTTP proxy services and can control which users are allowed to use which services. User accounts can be defined on the security system, through the **Definitions/ Users** menu. Or on an external user database. Supported external databases include **RADIUS**, **SAM** (Windows NT/Windows 2000/XP-Server), **Microsoft Active Directory** and **OpenLDAP**. If an external user database is already present on the network, you can use it instead of having to re-enter user accounts on the security system itself.

User Authentication requires users to identify themselves before using network services. This allows for user-based access control and accounting rather than an IP-based access control. This allows for user-based **Accounting** in the HTTP-Proxy access protocol.

Proxy Service and Authentication Methods

The **SOCKSv5**, **SMTP**, and **HTTP** services can be configured to allow or disallow clients based on IP address or on username and password combinations. In order to use **User Authentication**, you must select at least one database against which the security system should authenticate users. If user authentication is enabled and no database is selected, the proxy service cannot be used.

The security system supports user authentication against ...

- A RADIUS Server
- An NT SAM user list
- An LDAP Server
- An internal database defined in WebAdmin

The four user databases can be checked one after the other.

Using the Security System

5.1.7.1. RADIUS

RADIUS stands for **Remote Authentication Dial In User Service** and is a protocol for allowing network devices (e.g., routers) to authenticate users against a central database. In addition to user information, RADIUS can store technical information used by network devices. Such as protocols supported, IP addresses, telephone numbers, routing information, and so on. Together this information constitutes a user profile that is stored in a file or database on the RADIUS server.

In addition to authenticating dial-up users, **RADIUS** can be used as a generic authentication protocol.

The RADIUS protocol is very flexible, and servers are available for most operating systems, including Microsoft Windows NT/2000. The RADIUS implementation on this security system allows you to configure access rights on the basis of proxies and users.

Before you can use **RADIUS** authentication, you must have a functioning RADIUS server on the network. As passwords are transferred in clear text (unencrypted), we strongly recommend that the RADIUS server be inside the network protected by the security system, and that the security system and server be on the same switch.

The following section details the setting up Microsoft IAS (RADIUS Server for MS Windows NT and 2000). If you use a different server, you will need the following information to enable the operation of the security system together with the user authentication.

The authentication request comprises three set fields:

- Username
- Password in clear text (PAP)
- Type of proxy (the string **http**, **smtp** or **socks**) in the **NAS-Identifier** field

Your RADIUS server should use this information to determine whether or not access should be granted, and should send back a properly formatted reply.

Configuring Microsoft's IAS RADIUS Server:

IAS is a part of all versions of Microsoft Windows 2000 Server, but is generally not installed by default. For Microsoft Windows NT4, **IAS** is a part of the **NT4 Option Pack** and is available without charge. The MS Windows NT4 IAS has fewer features than the 2000 version, but is nevertheless sufficient for user authentication with the security system.

1. Check that the **IAS** service is installed. If it is not, install it now.
2. Create a user group for every proxy to be used.

Tip:

Name the group according to the proxy to be used. For example, name the group for the HTTP Proxy **HTTP Proxy Users**.

3. For each group, add the users who should be allowed to use this proxy service.
4. Make sure that the user flag **Allow dial-in access to the network** is set for every user in these groups.
You can find this setting in the user properties dialog box. MS Windows NT/2000 needs this flag to answer RADIUS inquiries.
5. Open the administration program for the **IAS** service.
6. Add a client. This requires the following information.

Client Name: Enter the **DNS** name of your security system here.

Protocol: Choose **RADIUS**.

IP Address of the Client: Enter the internal IP address of the security system.

Using the Security System

Client Vendor: Choose **RADIUS Standard**.

Shared Secret: Enter a password here. You will need this password again when configuring the RADIUS server with **Web-Admin**.



Security Note:

For the **Shared Secret** only passwords consisting of alphanumeric, minus (-), and period (.) characters are allowed. Other characters, for example %!#{ } are not allowed.

7. Now open the **RAS rules** menu.

A standard rule is listed here. If you intend to use **IAS** only with the security system, you can delete this entry.

For every proxy, enter a rule. Choose a descriptive name, such as HTTP access.

Add two conditions:

1. Condition 1: The NAS Identifier field must correspond to a string from the following table.

Proxytyp	NAS-Identifer entspricht String
HTTP	http
L2TP over IPSec	l2tp
PPTP	pptp
SOCKS	socks
SMTP	smtp
WebAdmin Access	webadmin
Surf Protection	"Profilname"

2. Condition: The Windows group of the user must match the group established in step 2.

Access is granted only when both conditions are met.

Using the Security System

8. Edit the profile so that no unencrypted connection is allowed by disabling the **No Encryption** function in the **Encryption** register.
9. Edit the profile for the rule so that unencrypted authentication (PAP) is allowed.
Leave the other values unchanged.
10. Open the **WebAdmin** configuration tool and open the **User Authentication** menu in the **System** tab.
11. In the **RADIUS Server Settings** window, click the **Enable** button next to **Status** (the status light will show green).



Address or Hostname:

Enter the IP address or the host name of the RADIUS server.

Shared Secret: Enter the **Shared Secret** from step 6.

12. Click the **Save** button to save these settings.
13. In the **Proxies** tab, open the menu corresponding to the proxy service you wish to use.
14. If **User Authentication** is not enabled (red status light), click the **Enable** button.

Authentication Methods: Choose RADIUS from the selection field.

15. Now confirm your settings by clicking on the **Add** button.

The user authentication using **RADIUS** is now active.

The IAS service will log every access attempt in the Microsoft Windows NT/2000 **Event Log**.

In order to prevent the Windows Event Log from overflowing, the security system stores caches RADIUS access information for five

Using the Security System

minutes. This may mean that changes in the RADIUS database will not be reflected at the security system for a few minutes.

Attention:

The security system sends queries on UDP port 1812.

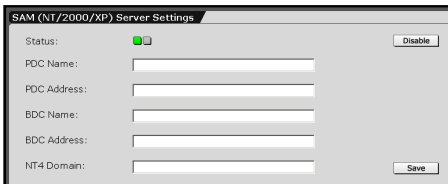
5.1.7.2. SAM - NT/2000/XP

This authentication method uses an MS Windows NT/2000 Domain Controller or standalone server. Many businesses already use MS Windows NT/2000 networks based on ActiveDirectory.

The advantage of SAM is that it is very easy to configure if the network already has a **Primary Domain Controller (PDC)** or if a server with a user database is running.

The drawback, however, is that this system does not distinguish between different user groups. You can either allow all users in an SAM database access to a proxy or none of them.

Configuring SAM – NT/2000/XP:



In order to use this authentication method, you will need to have a Microsoft Windows NT or 2000 server on your network that contains the user information. This can be either a

Primary Domain Controller (PDC) or a standalone server.

Note that Windows servers have a NetBIOS name (the NT/2000 server name) as well as an IP address.

1. In the **System** tab, open the **User Authentication** menu.

2. In the **SAM (NT/2000/XP) Server Settings** window, click the **Enable** button next to **Status**.

PDC Name: Enter the name of the Domain Controller in this entry field.

Since, beginning with Windows 2000, these names are also official DNS names, only names consisting of alphanumeric, minus (-), and period (.) characters are allowed.

Other characters, for example %!#_{ } are not allowed.

PDC Address: Enter the IP address of the Domain Controller.

BDC Name: If you have a Backup Domain Controller, enter its name in this entry field. If you do not use a BDC, enter the name of the PDC here.

BDC Address: If you have a Backup Domain Controllers, enter its IP address here. If you do not use a BDC, enter the name of the PDC here.

NT4 Domain: Enter the name of your MS Windows NT/ 2000-Domain.

Allowed characters are: Letters of the alphabet, digits from 0 to 9, hyphen, and underscore characters.

Note:

This is not the Internet domain, as in Company.com, but rather a simple designator, e.g., **Intranet**. If you are using a stand-alone server rather than a Domain Controller, enter its NETBIOS name here. This corresponds to the **PDC Name** entry.

3. Click the **Save** button to save these settings.
-



Security Note:

For the **Shared Secret** only passwords consisting of alphanumeric, minus (-), and period (.) characters are allowed. Other characters, for example %!#_{ } are not allowed.



Security Note:

If you use SAM authentication, make sure to disable the **Guest** account on your Windows domain. Otherwise all username/password combinations will be accepted as valid.

5.1.7.3. LDAP Server

LDAP, the **Lightweight Directory Access Protocol** defines the way in which clients communicate with X.500-conforming directory services. The protocol thus specifies the type of access to such a directory service.

The security system uses the **LDAP** protocol to authenticate users for several of its services. The security system allows or denies access on the basis of certain attributes or group memberships established on the LDAP server.

This system supports the **Microsoft Active Directory** and **Novell eDirectory** LDAP servers as well as those based on the Open Source **OpenLDAP** software.

Microsoft Active Directory is an indexing service designed especially for Windows NT/2000 networks, and allows the central management and organization of network resources. It allows users to access system resources after a single sign on to a central server, and offers administrators centrally organized management of users, regardless of network topology or protocols used.

In order to use this directory service, you will need an MS Windows NT/2000 Domain Controller.

Novell eDirectory – Novell Directory Service 8 - is an X.500-based index service designed to manage users, access rights, and other network resources. eDirectory is available for Netware versions 5 and higher, MS Windows NT/2000, Linux, and Solaris.

The **OpenLDAP Foundation**, the group which manages the **OpenLDAP** open source project, has released the Stand-Alone LDAP server, called SLAPD. OpenLDAP can also be used to build a networked directory service with various other LDAP servers: For instance, the **iPlanet Directory Server** from Sun Microsystems is based on OpenLDAP code and fully compatible.

User Authentication

LDAP uses the **Distinguished Name (DN)** of a user to identify him or her. This name must be unique within the directory.

Microsoft Active Directory (AD) and **Novell eDirectory (NDS8)** give every object a defined **DN**. This DN identifies the object uniquely in the AD index or NDS tree. This **DN** is composed of the **Common Name (CN)** and **Domain Component (DC)**.

Example: CN=Administrator, CN=Users, DC=example, DC=com

MS Active Directory also allows for user authentication by User **Principal Name (UPN)**. This name consists of the login name and DNS name of the domain.

Example: admin@example.com

OpenLDAP simply uses the **Common Name (CN)** to identify users. Please make certain that every user has a unique **CN**.



Security Note:

User authentication with a stand-alone LDAP server involves sending passwords in clear text over the network. As these passwords are not encrypted, an attacker with access to the network may be able to intercept them.

Using the Security System

Note:

User authentication with an **LDAP Server** requires that the **DNS Proxy** on the **Proxies/DNS** menu be enabled.

Configuring the Microsoft Active Directory Server:

Make sure that there is a user configured on your LDAP server to have full read privileges for the directory. This will be the query user.

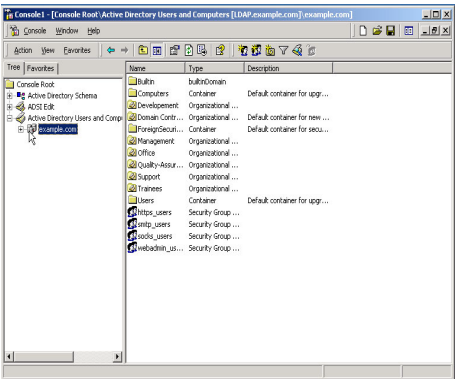


Security Note:

Make sure that the user has **only** read privileges.

Microsoft Active Directory (AD) can grant privileges on the basis of group memberships, or on the basis of particular user attributes. In most cases, it is easier to use the **Member Of** query type to authenticate by group.

The Directory can be extended by self-defined attributes. If you wish to authenticate on the basis of particular User Attributes, every user account in the directory must be edited to define access rights. This is done by setting a particular attribute for each user which either grants or denies access to a service.



The following example illustrates the configuration for a hypothetical small company **example.com**:

The user **John Smith** is in the **Trainees** directory.
DN: cn=john smith,
ou=trainees, dc=example,
dc=com.
LogonName:
smith@example.com

Using the Security System

This user can use his LogonName and password to log on to services like the SOCKS Proxy. The security system checks the user's DN and password. If there is only one DN that corresponds to smith@example.com, and if the supplied password is valid, the user will be allowed to use the SOCKS proxy.

If you wish to use **Group Membership** to control access rights, complete the following steps to configure the **Microsoft Active Directory**:

Step 1 – Creating a Security Group:

1. In the **Microsoft Management Console**, click the domain with the right mouse button.

Example: Domain **example.com**

2. With the left mouse button, click **New** and then **Group**.

A new window will open labeled **New Object - Group**.

3. Enter a unique name for the group in the **Group name** field.

Example: **socks_users** for the SOCKS Proxy

4. Under **Group type** select **Security**.

5. Save your settings by clicking **OK**.

You have now created a new **Security Group** named **socks_users**.

Step 2 – Adding Users to the Group:

1. In the directory, right-click the username.

Example: **John Smith** in the **Trainees** directory.

2. Left click the **Properties** button.

A window named **Properties** will open.

3. In the **Properties** window, select **Member Of** tab.

Using the Security System

4. Click **Add** to add the new group.

The **Select Groups** window will open.

5. Now choose the **Security Group** you wish to add the user to.

Example: **socks_users**

6. Save your changes by clicking **OK**.

The new **Security Group** will be added in the **Member Of** window.

7. Save your settings by clicking **OK**.

Now execute the settings on the Internet security system. The settings in the configuration tool **WebAdmin** are explained on page 87.

Microsoft Active Directory, self defined attributes:

User authentication with Microsoft Active Directory can also use user attributes to assign access rights. For large organizations, however, this can be time-consuming to configure.

Note:

According to the LDAP standard, each user attribute must have an associated **object ID, or OID**. Object ID numbers are designed to be unique across the entire Internet; in order to manage this, the **Internet Assigned Numbers Authority (IANA)** has been charged with assigning OID prefixes to organizations. For example, the OID prefix for Astaro AG is: 1.3.6.1.4.1.9789.

If your organization does not yet have an official OID space, you can request an OID prefix from the **IANA** at **www.iana.org**. Once you have an OID space, you should consider how best to use it to describe your network structure. Remember that each user attribute will require a unique OID.

In order to configure user attributes, the **Microsoft Management Console** must be used to modify the **Active Directory Schema**. In order to do this, you must first mark the schema as editable.

Step 1 – Enable Editing of the Active Directory Schema:

1. In the **Microsoft Management Console**, right-click **Active Directory Schema**.
2. Use the left mouse button to click **Operations Master**.
The **Change Schema Master** window will open.
3. Check the option **The Schema may be modified on this Domain Controller**.
4. Save your changes by clicking **OK**.

The **Active Directory Schema** can now be edited.

Step 2 – Add New Attributes:

1. Under **Active Directory Schema**, right click **Attribute**.
2. Use the left mouse button to click **New**.
3. In the **Create New Attribute window**, define the new attribute.

Common Name: Enter a **CN** for this attribute.

LDAP Display Name: Give the new attribute a clear label. The name of the service this attribute controls would be a good choice.

Example: **Socks**.

Unique X500 Object ID: Enter the OID for this attribute in the entry field.

Syntax: Chose **Boolean**.

Minimum: Leave this field blank.

Using the Security System

Maximum: Leave this field blank.

4. Save your settings by clicking **OK**.

Step 3 – Allocate a Class for the Attribute:

1. Under **Active Directory Schema**, left-click **Classes**.
2. Right-click **Users**.
A window named **User Properties** will open.
3. Click the **Attributes** tab and make the following settings.
Optional: Use the drop-down menu to select the attribute and click **Add**.
4. Save your settings by clicking **OK**.
5. In the **Microsoft Management Console**, right-click **Active Directory Schema**.
6. With the left mouse button, click **Reload the Schema**.

Step 4 – Setting the Attribute for Users:

1. In the **ADSI Edit** window, right-click the user to edit.
Example: **John Smith** in the **Trainees** directory.
2. Left click the **Properties** button.
A window named **Properties** will open.
3. In the **Properties** window, click the **Attributes** tab.
4. **Select which properties to view:** Choose **Both**.
5. **Select a property to view:** Choose the attribute to set.
Example: **Socks**.
Syntax: This value was set while creating the attribute and cannot be changed.
From step 2, this should be. **Boolean**.

Edit Attribute: You can use this field to set the value of the attribute. The possible values are **TRUE** and **FALSE**.

Value(s): The current value of the attribute is shown here.

6. Save your settings by clicking **OK**.

Now make the settings on the Internet security system. The settings in the configuration tool **WebAdmin** are explained on page 87.

Configuring a Novell eDirectory Server:

Make sure that there is a user configured on your LDAP server to have full read privileges for the directory. This will be the query user.



Security Note:

Make sure that the user has **only** read privileges.

In most cases, you should use the **groupMembership** query type with **Novell eDirectory (NDS8)**, as this allows an existing user index to be easily extended for proxy rights.

The index can also be configured to use user-defined attributes, which must be manually set for each user in the index. If you wish to authenticate on the basis of particular User Attributes, every user account in the directory must be edited to define access rights. This is done by setting a particular attribute for each user which either grants or denies access to a service.

You will need **Novell ConsoleOne** to configure the eDirectory Server.

The configuration and management of the Novell eDirectory server is described in detail in the accompanying documentation. You can find these documents at:

<http://www.novell.com/documentation/lg/edir87/index.html>

Then make the settings for the Internet security system. The settings in the configuration tool **WebAdmin** are explained on page 87.

Using the Security System

Configuring the OpenLDAP Server:

Make sure that there is a user configured on your LDAP server to have full read privileges for the directory. This will be the query user.



Security Note:

Make sure that the user has **only** read privileges.

With **OpenLDAP**, users are identified on the basis of their **Common Names (CN)**. Please make certain that every user has a unique **CN**.

Important Note:

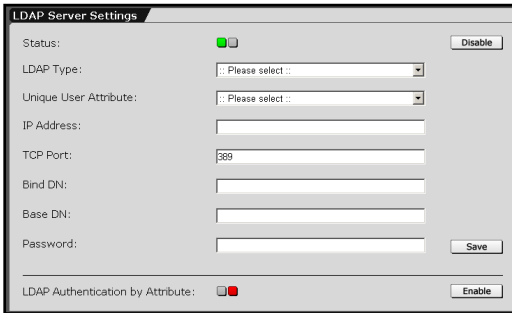
With the installation of the software all existing data will be deleted from the computer!

Because there are many different LDAP servers based on the **OpenLDAP** code, it is impossible to describe them all here. For further information, please consult the documentation accompanying your LDAP server.

If you are using the **SLAPD** server from the **OpenLDAP Foundation**, the current documentation is available at:

<http://www.openldap.org>.

Configuring LDAP on your Security System:



Make sure that there is a user configured on your LDAP server to have full read privileges for the directory. This will be the query user.

You will need the **Distinguished Name (DN)** of this user as well as the IP

address of your LDAP server in order to complete the configuration of the security system.



Security Note:

Make sure that the user has only read privileges.

1. In the **System** tab, open the **User Authentication** menu.
2. In the **LDAP Server Settings window**, enable the system by clicking **Enable** next to **Status**.

LDAP Type: Choose the type of LDAP server to use.

The available choices are: **Microsoft Active Directory**, **Novell eDirectory** and **OpenLDAP**.

Unique User Attribute: This attribute defines how users should be authenticated on the LDAP server. The attributes available here depend on the type of LDAP server you are configuring. If you wish to use a self-defined attribute for authentication, select **Selfdefined** here.

With the **Microsoft Active Directory** server, you can also choose to authenticate by **User Principle Name (UPN)** or **saMAccountName**.

Using the Security System

The **Novell eDirectory** and **OpenLDAP** servers allow authentication by the **Common Name (CN)**, **Surname (SN)**, and **Unique Identifier (UID)** attributes.



Attribute Name: This entry field is only shown if you have selected to authenticate by a **Selfdefined** attribute from the **Unique User Attribute** drop-down menu.

Enter the attribute to use for authentication here.

IP Address: Enter the IP address of the LDAP server.

TCP Port: Enter the TCP port of the LDAP service. By default, this is set to 389 (the standard port for LDAP).

Bind DN: The value to enter here depends on the type of LDAP server you are using.

1. Microsoft Active Directory

Microsoft Active Directory can use either the **User Principal Name (UPN)** or the full **Distinguished Name (DN)** of the user.

Examples:

UPN: admin@example.com

DN: cn=administrator, cn=users, dc=example, dc=com

2. Novell eDirectory

Enter the full **Distinguished Name (DN)** of the user.

Example:

DN: cn=administrator, o=our_organisation

3. OpenLDAP

OpenLDAP and OpenLDAP-conforming servers can only use the **Distinguished Name (DN)** of users.

Base DN: Enter the object name to be used as the basis for all client actions.

Examples:

For MS Active Directory: dc=example, dc=com

For Novel eDirectory: o=our_organisation

7. Enter the password in the **Password** entry field. This password should also be used for the Administration of the Stand-alone-LDAP-Server.



Security Note:

Use a secure password! Your name spelled backwards is, for example, not a secure password – while something like xFT35\$4 would be.

-
8. Click the **Save** button to save these settings.



Security Note:

As long as the **LDAP authentication by attribute** function is disabled, all users who are listed in the directory with a unique **DN** and a valid password can use the **HTTP**, **SMTP** and **SOCKS** proxies, and can also access the **WebAdmin** tool.

Advanced Authentication with LDAP:

1. Enable the **LDAP authentication by attribute** function by clicking **Enable** next to **Status**.

2. Use the **Service** drop-down menu to select a service.

The available services are: **HTTP**, **SMTP**, **SOCKS** and **Web-Admin**.

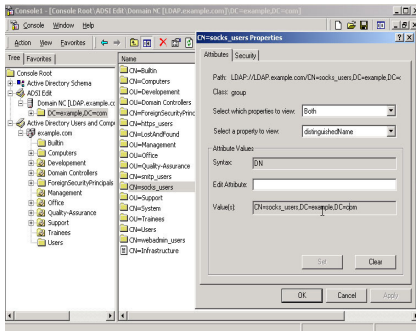
3. In the **Attribute Name** field, enter the name of the attribute.

If you are using authentication using the **MemberOf** property on a **Microsoft Active Directory** Server, this should be the name of the **Security Group** to use.

Example: **socks_users**.

Using the Security System

4. In the **Attribute Value** field, enter the **DN** for the attribute. The attribute value is the **DN**.



Microsoft Active Directory displays the **DN** of attributes in the **Management Console**, under **ADSI Edit**:

Here, under the **Base DN** (example: dc=example, dc=com), find the attribute name (example: socks_users) and right-click it. A window labeled **CN=socks_users Properties** will open.

Use the **Select which properties to view** drop-down menu to choose **Both**, and in the **Select a property to view** drop-down menu, choose **distinguishedName**. The **DN** for this attribute will be shown in **Value(s)**.

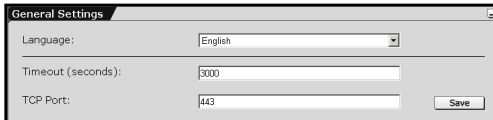
5. Click the **Save** button to save these settings.

Every member defined as a **MemberOf** the security group **socks_users** will be allowed to use this service.

5.1.8. WebAdmin Settings

Configure the access to the **WebAdmin** configuration tool in this menu.

General Settings



Language: In this drop-down menu you can determine the language.

Timeout (seconds): In this entry field enter the intervals in seconds, in which **WebAdmin** automatically logs you out, if there are no actions. By default, the system is set to 300 seconds after the installation. The smallest possible interval amounts to 60 seconds.

Click the **Save** button to save these settings.

If you close your browser with an open **WebAdmin** session without closing **WebAdmin** through **Exit**, the last session remains active until the end of the time-out.

TCP Port: If you want to use the standard port 443 for the HTTPS service for another purpose (such as a deviation with **DNAT**), you must enter another TCP Port for the **WebAdmin** Interface here. Possible values are 1024-65535, while certain ports are reserved for other services. In order to address **WebAdmin** after a modification, you must separately link the port through a colon to the IP-address of the Internet security system, e.g.: `https://192.168.0.1 :1443`.

Using the Security System

Access and Authentication

The screenshot shows the 'Access and Authentication' configuration window. It contains three main sections: 'Allowed Networks', 'Authentication Methods', and 'Allowed Users'. In the 'Allowed Networks' section, 'Any' is selected in the 'Selected' list, and the 'Available' list contains 'Bookkeeping', 'Development', 'FTP Server', 'Internal (Address)', and 'Internal (Broadcast)'. In the 'Authentication Methods' section, 'Local Users' is selected in the 'Selected' list, and the 'Available' list is empty. In the 'Allowed Users' section, 'admin' is selected in the 'Selected' list, and the 'Available' list is empty. At the bottom, there is a 'Log Access Network Traffic' checkbox (checked) and an 'Enable' button.

Allowed Networks: Add those networks to the selection field that are authorised to access **WebAdmin**. As with **SSH**, **Any** is entered here for a smooth installation. In this case and if the password is available, **WebAdmin** can be accessed from everywhere.

Security Note:

As soon as you can limit the access to the Internet security administration (for example your IP address in the local network), replace the **Any** entry in the **Allowed Networks** selection field through a smaller network.

The safest solution is, if only one administrator PC has access to the Internet security system through HTTPS.

Networks can be defined in the **Definitions/Networks** menu.

Authentication Methods: Select the authentication method in the selection field. In order to give you access to the Internet security system through the configurations tool **WebAdmin** after the installation, the authentication method **Local Users** has already been defined here and the respective **User** has been entered in the **Allowed Users** selection menu.

Further available authentication methods are **NT/2000/XP Server**, **RADIUS Database** and **LDAP Server**.

Local **Users** are administered in the **Definitions/Users** menu.

Allowed Users: By default this is set to the user **admin**.

Local users are defined in the **Definitions/ Users** menu.

Log Access Network Traffic: All connections to the **WebAdmin** configuration tool are logged to the **Packet Filter Logs** as **Accept** rule. The **Packet Filter Logs** can be found in the **Local Logs/ Browse** menu. By default, this function is disabled.

Enable this function by clicking on the **Enable** button (status light on green).

Block Password Guessing



This function can be used to limit the number of attempts to log in to the **WebAdmin** configuration tool. After a specific number of attempts, the access from this IP address will be denied for a

given time span.

Configuring the blocking protection for Login attempts:

1. Configure the maximum allowable number of attempts in the **After failed Attempts** drop-down menu.
2. Enter the time span for the blocking protection in the **Block IP for Period** entry field.
3. Save your changes by clicking **Save**.

Now, the blocking protection is enabled. The **Never block Networks** window, allows you to exclude networks or hosts from the blocking protection.

Using the Security System

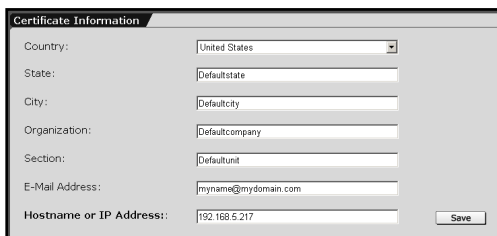
5.1.9. WebAdmin Site Certificate

Encryption systems are an important part of many modern security systems. They are used, for example, when transmitting confidential information over **Virtual Private Networks** (in chapter 5.7 on page 260), in **user authentication** and **Up2Date Service** or, to securely administer the security system over the network.

Certificates and Certificate Authorities (CA) are an essential part of modern cryptographic protocols, and help close the gaps left open by other systems. **Public Key** Algorithms offer a particularly elegant form of encryption. They do, however, presuppose that the public keys of all communications partners are known.

At this point, a third, trusted party is used to ensure the validity of public keys. The third party issues certificates guaranteeing the authenticity of these keys: this third party is called a **Certificate Authority (CA)**. A certificate is a record in a standardized format with the owner's most important data - his name, and his public key - and is signed with the private key of the **CA**. The format for these certificates is defined in the X.509 standard.

In a certificate, the **CA** certifies, with its own signature, that the public key belongs to the person (or entity) it says it does. As the certificate contains information such as the name of the owner, duration of validity, issuing authority, and the signature of the CA, it can be seen as a kind of digital passport.



The screenshot shows a web form titled "Certificate Information". It contains several input fields with default values: Country (United States), State (Defaultstate), City (Defaultcity), Organization (Defaultcompany), Section (Defaultunit), E-Mail Address (myname@mydomain.com), and Hostname or IP Address (192.168.5.217). A "Save" button is located at the bottom right of the form.

Country:	United States
State:	Defaultstate
City:	Defaultcity
Organization:	Defaultcompany
Section:	Defaultunit
E-Mail Address:	myname@mydomain.com
Hostname or IP Address:	192.168.5.217

Save

The **WebAdmin Site Certificate** menu allows you to create two certificates: first a CA certificate, which will be installed in your browser, and second the server certificate (signed by the CA

certificate) which the system uses to authenticate itself to your browser. These two certificates contain the company's data and the system's hostname.

Creating a Certificate for WebAdmin:

1. Under the **System** tab, open the **WebAdmin Site Certificate** menu.
2. In the **Certificate Information** menu, enter the appropriate information for your firm.
Country: Choose your country from the drop-down menu.
State: Choose the state or region where you are.
City: Enter the company's name.
Organization: Enter the company's name.
Section: Enter the department.
E-Mail Address: Enter your e-mail address.
3. In the field **Firewall Hostname**, enter the host name or IP address of the firewall you use to access **WebAdmin**.
Example: If you access **WebAdmin** through the URL `https://192.168.10.1`, enter 192.168.10.1 here.
4. Save your entries by clicking the **Save** button.

Installing a Certificate for WebAdmin:

1. To install the CA Certificate in your browser, click **Import Certificate into Browser** in the **CA Certificate Installation** window

The next few steps depend on your browser. For example, with Microsoft Internet Explorer, the **File download** dialog opens.

Save file to disk: This option allows you to save the certificate to a local disk before installing it.

Using the Security System

Open the file from current position: This allows you to install the certificate directly. The **Certificate** window will open. These registers allow you to inspect the information contained in the certificate before installing it.

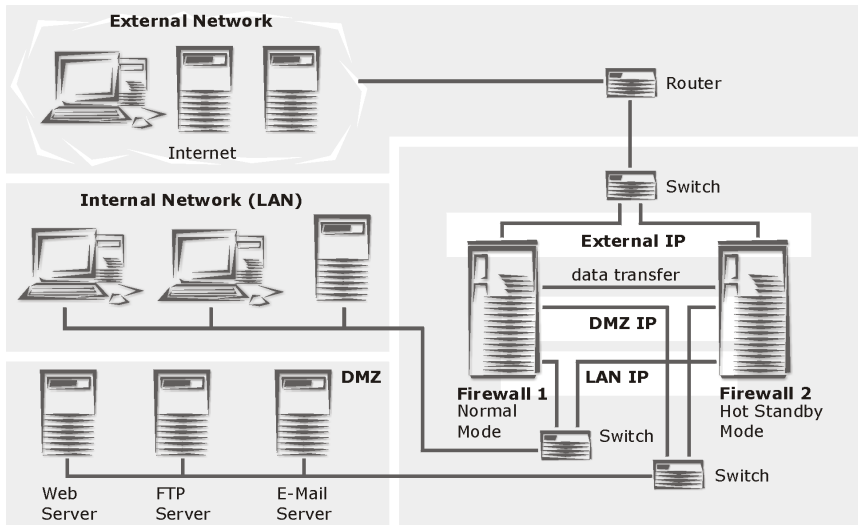
5. Click the **OK** button to start the process.
-

Note:

Due to system time differences and timezone offsets, the generated certificate may not yet be valid. Many browsers wrongly report that such certificates have expired, however this is not the case and any generated certificates will become valid after a maximum of 12 hours.

5.1.10. High Availability

The main cause of system failure is hardware failure, such as a failure of the network card, hard disk, or processor. The **High Availability (HA)** option allows you to use two systems with identical hardware in parallel. The first system runs normally (master mode), while the second runs in standby (slave) mode, monitoring the active system over the data transfer link using the link beat. The standby system also receives periodic updates over this link so that, in the case of system failure on the primary, it can take over operations immediately.



Hardware and Software Requirements

- The High Availability (HA) License
- 2 security systems with identical hardware
- 2 additional Ethernet interfaces (if you wish to use heartbeat monitoring, both of these must support link-beat)
- One Ethernet crossover cable
- One serial interface cable (optional)

Using the Security System

Important Note:

The hardware components, supported by the Internet security system, e.g. for a monitoring through Heart-Beat-requests are listed under **<http://docs.astaro.org>** in the **Hardware Compatibility List for Astaro Security Linux** tab.

Installing the High Availability-System

Preparation:

1. First install the software on both machines and configure the first (active) system as described in chapter 3.2 on page 22.
-



Security Note:

If you install **High Availability (HA)** to a system updated using Up2Date, please ensure that the standby system is using the same version of the security solution as the normal-mode system.

2. Shut both systems down.
3. Connect the firewall system 2 (standby) to the firewall system 1 (active) as in the graphic.

Configuring the Firewall System 1 (normal mode):

1. Start system 1 as normal.
2. In the **System** tab, open the **High Availability** menu.
3. Enable the HA system by clicking **Enable** (under **Status**).

Device Name: Enter a descriptive name for the system here. This name will be shown to allow you to know which system is active at a given time. The name can be up to 11 characters long.

Device IP: Assign an IP-address from a Class-C-network to each security system within the HA-device group. The IPs must be within an address range and may only be used once within a given device group. Example: The *Device IP 10.0.0.1* is assigned to the *Internet security system 1* and the *Device IP 10.0.0.2* to *security system 2*.

Encryption Key: Enter a password here.



Security Note:

Use a secure password! Your name spelled backwards is, for example, not a secure password – while something like xft35\$4 would be.

Network Interface Card: Select a network card to be used for the data transfer connection. When an interface is selected for HA mode, it cannot be used in any of the other configuration menus.

Important Note:

The network cards used for the connection must have the same **Sys ID** (e.g., eth3) on both systems.

If you wish to use heartbeat monitoring, use this menu to choose network cards on both the normal and standby systems which support link beat.

Transfer Network: Enter the **Network Address** for the data transfer connection here.

Note:

Note: The data transfer connection must use a Class C network – that is, a network with mask 255.255.255.0. The bitmask form cannot be used.

The data transfer network cannot be used for anything other than data transfer.

Using the Security System

The entry fields contain suggestions generated by the system. You do not need to accept the default values.

Serial Interface (optional): In addition to watching the data connection, the standby system can monitor the active system through the serial interface. No data is transferred over this connection. Use the drop-down menu to select the appropriate serial interface to use this option.

Note:

When you save the settings, according to the following instructions, the system will shut down and reboot immediately.

4. Click the **Save** button to save these settings.

The first system will shut down and reboot immediately. If you have connected a keyboard to this machine, the **Num Lock** light will flash.

When the system is in Hot Standby Mode, it will beep twice and the LED display will stop blinking. Because system 2 is still disabled, the first system will boot normally into normal mode, and the **Num Lock** light will continue to blink.

After system 1 completes the boot process, the **Num Lock** light will stop blinking, and the system will beep five times: This signals that the middleware has successfully loaded and initialized all services, rules, and processes.

Note:

If the beeps are not heard, and the LED light continues to blink, the middleware was unable to initialize all services, rules, and processes. If this happens, please contact the service department of your security solution supplier.

Configuring System 2 (Hot Standby Mode):

1. Start system 2 as normal.
2. Complete steps 3 through 6 as above, and click **Save**.

The system 2 will now shut down and reboot immediately. If you have connected a keyboard to this machine, the **Num Lock** light will flash.

When the system is in Hot Standby Mode, it will beep twice and the LED display will stop blinking. System 2 recognizes system 1 through the data connection, and remains in Hot Standby Mode.

The **High Availability** system is now active.

System 2 will be updated at regular intervals over the data transfer connection. Should the active system encounter an error, the standby system will immediately and automatically change to normal mode and take over the system's functions.

Using the Security System

5.1.1.1. Shut down/Restart

Restart will shut the system down completely and reboot. Depending on your hardware and configuration, a complete **Restart** can take up to 5 minutes.

Restart:

1. Under the **System** tab, open the **Shut down/Restart** menu.
2. In the **action** drop-down menu, choose **Restart**.
3. Begin the reboot by clicking **Start**.
4. When asked **Do you really want to restart?**, click **OK**.

The action **Shut down** allows you to shut the system down, and allows you to cleanly stop all running services.

For systems without a monitor or LCD display, the end of the shut down process is signaled by an unending series of beeps at one-second intervals.

Depending on your hardware and configuration, this process can take up to 5 minutes. Only after the system has completely shut down, signaled by the **Power down** message, should you turn off the power. If the system is turned off without being shut down properly, the system must check the consistency of the file system: this means that the next boot will take longer. In the worst case, data may be lost.

The system will beep five times in a row to signal a successful startup.

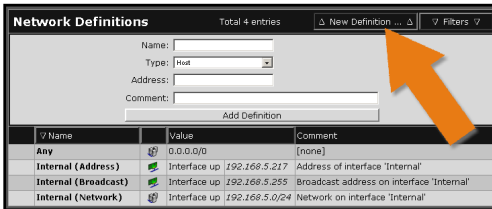
Shut down:

1. Under the **System** tab, open the **Shut down/Restart** menu.
2. In the **Action** drop-down menu, choose the **Shut down** action.
3. Begin the shutdown by clicking **Start**.
4. When asked **Do you really want to shut down?**, click **OK**.

5.2. Networks and Services (Definitions)

The **Definitions** tab allows you to define networks and services for all of the other configuration menus (e.g., the packet filter, VPN, proxies, etc.) in one central location. This allows you to work with the names you define, rather than struggling with addresses, ports, and network masks. Another advantage is, that can group individual networks and services together and configure them all at once. If, at a later date, you assign certain settings to these groups, they will apply to all networks and services contained therein. It is even possible to make groups of groups. Local users for the proxy services can also be defined here.

5.2.1. Networks



Network Definitions Total 4 entries [+ New Definition ...](#) [Filters](#)

Name:
 Type:
 Address:
 Comment:
[Add Definition](#)

Name	Value	Comment
Any	0.0.0.0/0	[none]
Internal (Address)	Interface up 192.168.5.217	Address of interface 'Internal'
Internal (Broadcast)	Interface up 192.168.5.255	Broadcast address on interface 'Internal'
Internal (Network)	Interface up 192.168.5.0/24	Network on interface 'Internal'

In the **Networks** menu, the hosts and networks and also the network groups are defined.







The network table contains static networks which have been pre-defined. By default, the table contains next to the definitions for the internal network card eth0 additional statically entered networks. These statical networks cannot be edited or removed. The hosts and networks can be grouped together. These groups will be treated as individual hosts and networks and can belong to an upstream group. The network types are represented by symbols.

The following pages contain a description of the different network types available and of how they are defined.

Using the Security System

The network types are represented by symbols:

The Symbols

Icon	Spalte	Anzeige/Einstellung
	Network type	Interface
	Network type	Host/Server
	Network type	Network
	Network type	Network group
	Network type	DNS server
	Network type	IPSec user group

Adding Host:

1. Under the **Definitions** tab, open the **Networks** menu.
2. Click on the New Definition button.
3. The entry window will open.
4. Make the following settings:

Name: In the entry field, enter a unique host name.

This name will be used later, for example to configure packet filter rules. Allowed characters are: The only allowed characters are alphanumeric characters, minus (-), space (), and underscore (_). Names may be up to 39 characters long.

Type: Select **Host** from the drop-down menu.

Address: Enter the IP-address in the entry field.

Comment: You can enter a host description in this entry field.

5. Save the host by clicking on the **Add Definition** button.

If the definition is successful, the new **Host** will be entered in the network table. You will now find this host under its name also in

different other menus. You could, for example define this host under **System/Remote Syslog** as **Remote Syslog Server**.

Adding Network:

1. Under the **Definitions** tab, open the **Networks** menu.

2. Click on the **New Definition** button.

The entry window will open.

3. Make the following settings:

Name: In the entry field, enter a network name.

This name will be used later, for example to configure packet filter rules. Allowed characters are: The only allowed characters are alphanumeric characters, minus (-), space (), and underscore (_). Names may be up to 39 characters long.

Type: Select **Network** from the drop-down menu.

Address/Netmask: Enter the IP address in the entry field and select the network mask from the drop-down menu.

Comment: You can enter a network description in this entry field.

4. Save the network by clicking on the **Add Definition** button.

WebAdmin will check that your entries are valid.

After successful definition, the new **network** will appear in the network table. The network name will also be available for use in various configuration menus.

Using the network name you can, for instance, enable HTTP proxy access for the new network under **Proxies/HTTP**.

Using the Security System

Adding DNS Server:

1. Under the **Definitions** tab, open the **Networks** menu.

2. Click on the **New Definition** button.

The entry window will open.

3. Make the following settings:

Name: In the entry field, enter a unique DNS Server name.

This name will be used later, for example to configure packet filter rules. Allowed characters are: The only allowed characters are alphanumeric characters, minus (-), space (), and underscore (_). Names may be up to 39 characters long.

Type: Select **DNS Hostname** from the drop-down menu.

Hostname: Enter the hostname in this entry field.

Comment: You can enter a DNS Server description in this entry field.

4. Save the host by clicking on the **Add Definition** button.

If the definition is successful, the new **Host** will be entered in the network table. You will now find this host under its name also in different other menus.

Defining Network Group:

1. Under the **Definitions** tab, open the **Networks** menu.

2. Click on the **New Definition** button.

The entry window will open.

3. Make the following settings:

Name: In the entry field, enter a unique network group name.

This name will be used later, for example to configure packet filter rules. Allowed characters are: The only allowed characters

are alphanumeric characters, minus (-), space (), and underscore (_). Names may be up to 39 characters long.

Type: Select **Network Group** from the drop-down menu.

Initial Members: From the selection field, select the network card by pressing the **Ctrl**-key on the keyboard and selecting the name with the mouse.

Comment: You can enter a network group description in this entry field.

4. Save the network group by clicking on the **Add Definition** button.

After successful definition, the new **network group** will appear in the network table. The network group name will also be available for use in various configuration menus.

Defining IPsec user group: .

This definition contains only the **Distinguished Name (DN)**. It is used for incoming IPsec-connections, using X.509 certificates. If the DN of the group corresponds to the one of the user, his virtual IP-address will dynamically be added to the group.

1. Under the **Definitions** tab, open the **Networks** menu.
2. Click on the **New Definition** button.

The entry window will open.

3. Make the following settings:

Name: In the entry field, enter a unique name for the IPsec user group.

This name will be used later, for example to configure packet filter rules. Allowed characters are: The only allowed characters are alphanumeric characters, minus (-), space (), and underscore (_). Names may be up to 39 characters long.

Type: Select **IPsec User Group** from the drop-down menu.

Using the Security System

DN Template: For the VPN-ID-Type **Distinguished Name** you will need the following data from the X.509 tab tree: Country (C), State (ST), Local (L), Organization (O), Unit (OU) Common Name (CN) and E-Mail Address (E).

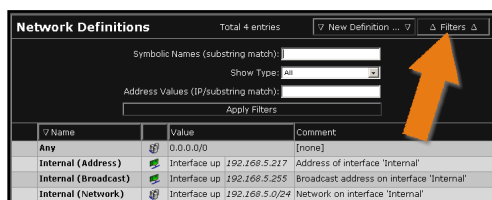
The data must be listed in the same order as a certificate in this entry field.

Comment: You can enter a IPsec user group description in this entry field.

4. Save the IPsec user group by clicking on the **Add Definition** button.

After successful definition, the new **IPSec user group** will appear in the network table. The IPSec user group name will also be available for use in various configuration menus.

Filters



The **Filters** function allows you to filter *networks* or hosts with specific attributes from the table. This function considerably enhances the management of huge net-

works, as networks of a certain type can be presented in a concise way.

Filtering networks:

1. Click on the **Filters** button.

The entry window will open.

2. Enter the filter attributes in the fields listed. You don't have to define all attributes.

Using the Security System

Name: If you want to filter the networks by names, enter the expression in the entry menu.

Type: Use this drop-down menu to filter the networks of a specific type.

Address Values: If you wish to filter networks by specific addresses, enter the IP-address in this entry field.

3. To start the filter, click on the **Apply Filters** button.

Only the filtered networks will be displayed in the table. Next time when you open the menu, the complete network table will be displayed.

Further Functions

Editing Definitions : Click on the settings in the **Name**, **Value** and **Comment** columns in order to open an editing window. You can then edit the entries.

Deleting Definitions: Clicking on the symbol of the trash will delete the definition from the table.

Using the Security System

5.2.2. Services

Name	Protocol	Source Port	Destination Port	Comment
Any		All protocols and services		Any - matches any service
AUS	TCP	1:65535	222	static
BGP	TCP	1024:65535	179	static
CITRIX	TCP	1024:65535	1494	static
DNS	TCP/UDP	1:65535	53	static
EUDORA	TCP	1024:65535	106	static
FTP	TCP	1024:65535	20:21	static
FTP-CONTROL	TCP	1024:65535	21	static
HBCI	TCP	1024:65535	3000	static
HTTP	TCP	1024:65535	80	static
HTTPS	TCP	1024:65535	443	static
IDENT	TCP	1024:65535	113	static
IMAP	TCP	1024:65535	143	static

The **Services** menu is used to define the Services and Service Groups.

Services define certain types of traffic over networks like the Internet. A service is defined by a **name**, a **protocol**, and **ports**.

The following protocols can be used: *TCP*, *UDP*, *TCP/UDP*, *ICMP*, *ESP*, *AH* and *IP*.

UDP uses port numbers between 0 and 65535 (inclusive) and is a stateless protocol that uses no so-called ACK-Bit. Because it does not keep state, UDP can be faster than **TCP**, especially when sending small amounts of data. This statelessness, however, also means that **UDP** cannot recognize when packets are lost or dropped. The receiving computer does not signal the sender when it receives packets successfully.

TCP connections also use port numbers from 0 to 65535 (inclusive). Lost packets can be recognized through *TCP* and be requested again. In a *TCP* connection, the receiver notifies the sender when a packet is successfully received (connection related protocol). *TCP* sessions begin with a **three way handshake** and are torn-down at the close of the session.

The **ESP** and **AH** protocols are used for **Virtual Private Networking (VPN)**. These protocols are covered in chapter 0 on page 258.

The network table contains the defined services and groups. By Default, the table contains the already pre-defined statically entered services.

Services can be grouped into **Service Groups**. These service groups can be used the same way single services can, and can themselves be included in other service groups. In the service table service groups are labeled by the group symbol (**--**).

The definition of *Service Groups* is described on page 112.

Add Service:

1. Under the **Definitions** tab, open the **Service** menu.
2. Click on the **New Definition** button.

The entry window will open.

3. Make the following settings:

Name: In the entry field, enter a unique **Service** name.

This name will be used later, for example to configure packet filter rules. Allowed characters are: The only allowed characters are alphanumeric characters, minus (-), space (), and underscore (_). Names may be up to 39 characters long.

Type: Select **Service** from the drop-down menu.

Protocol: Select the **Protocol** from the drop-down menu.

Source/Destination Ports: In the left entry menu, enter the Source Port, that is the Client Side of the service. In the right entry menu, enter the Destination Port, that is the Server Side of the service.

4. The other settings depend on the selected protocol:

For the **TCP** and **UDP** protocols you need the following two values. Entry options: A single port (e.g. 80) or a port range (e.g. 1024:64000).

Using the Security System

Source/Destination Ports: In the left-hand entry menu, enter the Source Port, i.e. the Client Side of the service. In the right hand entry menu, enter the Destination Port, i.e. the Server Side of the service.

The **ESP** and **AH** protocols are used for **IPsec VPN** connections. The port entered here should be agreed upon with the remote end of the IPSec VPN tunnel.

SPI: Enter a value from 256 to 65535. Values up to and including 255 are reserved by the **Internet Assigned Numbers Authority (IANA)**.

For the **ICMP** protocol, select a type of ICMP packet from the **ICMP type** drop-down menu.

For the **IP** protocol enter the protocol number into the **Protocol Number** entry field.

Comment: You can enter a service description in this entry field.

5. Save the **Services** by clicking on the **Add Definition** button.

After successful definition, the new service will appear in the service table.

Defining Service Group:

1. Under the **Definitions** tab, open the **Service** menu.
2. Click on the **New Definition** button.

The entry window will open.

3. Make the following settings:

Name: In the entry field, enter a unique **Service Group** name.

This name will be used later, for example to configure packet filter rules. Allowed characters are: The only allowed characters are alphanumeric characters, minus (-), space (), and underscore (_). Names may be up to 39 characters long.

Type: Select **Service Group** from the drop-down menu.

Initial Members: From the selection field, select the services by pressing the **Ctrl**-key on the keyboard and selecting the name with the mouse.

4. Save the **Service Group** by clicking on the **Add Definition** button.

After successful definition, the new service group will appear in the service table.

Filters

The **Filters** function allows you to filter *Services* with specific attributes from the table. This function considerably enhances the management of networks with many services, as services of a certain type can be presented in a concise way.

Filtering services:

1. Click on the **Filters** button.

The entry window will open.

2. Enter the filter attributes in the fields listed. You don't have to define all attributes.

Name: If you want to filter the services by names, enter the expression in the entry menu.

Protocol: This drop-down menu allows you to filter the services by specific protocols.

Source Port: If you want to filter services by a specific source port, enter it in this entry field.

Destination Port: If you want to filter services by a specific target port, enter it in this entry field.

Comment: If you want to filter services by specific comments, enter the expressions in this entry field.

Using the Security System

3. To start the filter, click on the **Apply Filters** button.

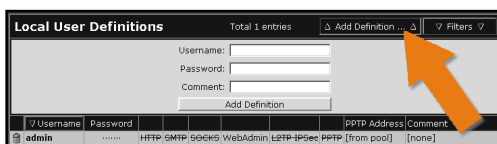
Only the filtered services will be displayed in the table. Next time when you open the menu, the complete service table will be displayed.

Further Functions

Editing Definitions: Click on the settings in the **Name**, **Value** and **Comment** columns in order to open an editing window. You can then edit the entries.

Deleting Definitions: Clicking on the symbol of the trash will delete the definition from the table.

5.2.3. Users



Username	Password	HTTP	SMTP	SOCKS	WebAdmin	L2TP-IPsec	PPTP	Address	Comment
admin							[from pool]	[none]

In the **Users** menu **Local Users** are added, if the use of proxy services should be limited to special persons.

This is an alternative to using an external user database. This menu allows you to define which user has access to which proxy services. Available options are **HTTP**-Proxy, **SMTP**-Proxy, **SOCKS**-Proxy, **WebAdmin**, **L2TP over IPsec** and **PPTP** (Remote Access).



Security Note:

Normally, only the **admin** user has access to **WebAdmin**. The password to WebAdmin should be changed at regular intervals.

Add Local Users:

1. Under the **Definitions** tab, open the **Users** menu.

2. Click on the **New Definition** button.

The entry window will open.

3. Make the following settings:

Username: In the entry field, enter a unique username for the local user.

This username will be used later, for example to configure packet filter rules. Allowed characters are: The only allowed characters are alphanumeric characters, minus (-), space (), and underscore (_). Names may be up to 39 characters long.

Password: Enter a password here.



Security Note:

Use a secure password! Your name spelled backwards is, for example, not a secure password – while something like xFT35\$4 would be.

Comment: You can enter a local user description in this entry field.

4. Save the **Local User** by clicking on the **Add Definition** button.

The new *User* will then be displayed in the table.

5. In the table, enable the services for the **Local User**.

At the beginning, no services are enabled for the user. Enable the services, by clicking on the corresponding term.

Example:

~~HTTP~~ = the HTTP Proxy is not enabled

HTTP = the HTTP Proxy is enabled

The available services are: **HTTP** Proxy, **SMTP** Proxy, **SOCKS** Proxy, **WebAdmin**, **L2TP over IPSec** and **PPTP** (Remote Access).

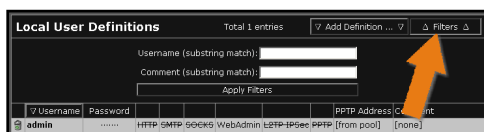
Using the Security System

PPTP Address: In PPTP connections also a static IP address can be assigned to a remote host instead of a dynamic address from a PPTP IP pool. In order to define a static IP, click on the field in the *PPTP Address* column and enter the address in the entry field.

Click the **Save** button to save your changes. In order to interrupt this process, click on the **Cancel** button.

For more information on **PPTP VPN Access**, please refer to chapter 5.3.6 on page 169.

Filters



The **Filters** function allows you to filter *Users* with specific attributes from the table.

This function considerably enhances the management of huge network configurations, as users of a certain type can be presented in a concise way.

Filtering users:

1. Click on the **Filters** button.

The entry window will open.

2. Enter the filter attributes in the fields listed. You don't have to define all attributes.

Username: If you want to filter the users by username, enter the expression in the entry field.

Comment: If you want to filter users by specific comments, enter the expressions in this entry field.

3. To start the filter, click on the **Apply Filters** button.

Using the Security System

Only the filtered users will be displayed in the table. Next time when you open the menu, the complete user table will be displayed.

Further Functions

Editing Local Users: Click on the settings in the **Name**, **Password**, **PPTP Address** and **Comment** columns in order to open an editing window. You can then edit the entries.

Deleting Local Users: Clicking on the symbol of the trash can will delete the definition from the table.

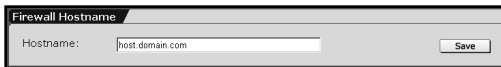
Using the Security System

5.3. Network Settings (Network)

The **Network** tab contains menus which allow you to configure **network cards** and **virtual interfaces**, as well as to perform network-specific configuration and management tasks.

5.3.1. Hostname/DynDNS

Firewall Hostname



Hostname: Enter the host-name for the security system in this entry field. Example: FIREWALL.mydomain.com

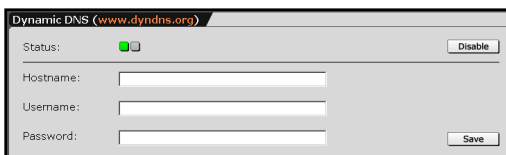
A Hostname or domain name may contain alphanumeric, period and minus characters. At the end there must be an alphabetic designator, such as „com“, „de“ or „org“. The **Hostname** will appear in the subject line of all **Notification E-Mails**.

Save your entries by clicking the **Save** button.

Note:

The **Hostname** will appear in the subject line of all **Notification E-Mails** to the Administrator.

Dynamic DNS



Dynamic DNS addresses a device or a VPN receiver through a DNS decryptable name. The respective applicable IP address is

stored for each name to a public DNS server in the Internet at each connection. The device can always be reached through this name - as

long as it online, at least. A mobile user, for example can access his company network through Dynamic DNS, even if the company only uses standard DSL connections with dynamic IP addresses. In addition to VPN applications, *Dynamic DNS* can also be used for remote maintenance and control.

Defining Dynamic DNS Servers:

1. In the **Network** tab, open the **Hostname/DynDNS** menu.
2. Enable the function by clicking on the **Enable** button in the **Status** column.

The entry window will open.

3. Make the following settings:

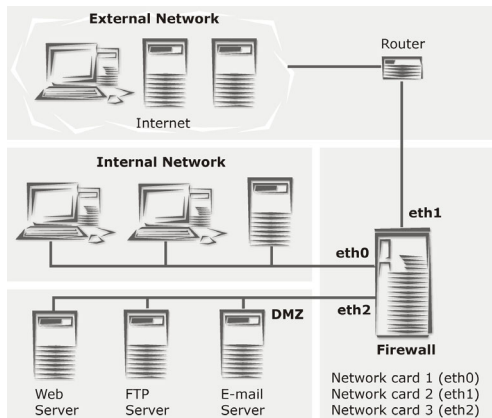
Hostname: In the entry field, enter the hostname.

Username: In the entry field, enter the username.

Password: In the entry field, enter the password.

4. Save your settings by clicking on the **Save** button.

5.3.2. Interfaces

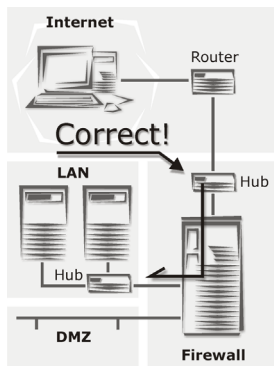


A firewall requires at least two **network cards** in order to securely connect an internal network (LAN) to an external one (the Internet). In our examples, the **Network card eth0** is always the interface connected to the internal network. **Network card eth1** is the interface connected to the external network (e.g., to

Using the Security System

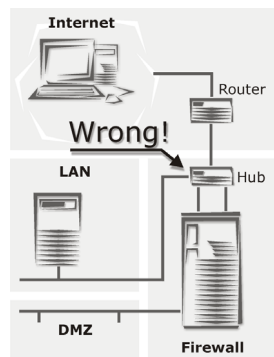
the Internet). These interfaces are also called the **trusted** and **untrusted** interfaces, respectively.

Network cards are automatically recognized during the installation: if new network cards are added later, a new installation will be necessary. In order to re-install the system, simply make a backup of your configuration, install a new copy of the software, and re-load your backed-up configuration.



As is shown in the graphic at left, the firewall must be the only point of contact between internal networks and external ones. All data must pass through the security system.

We strongly recommend against connecting both internal and external interfaces to one hub or switch – except if the switch is



configured as a VLAN switch. There might be wrong ARP resolutions (Address Resolution Protocol) (ARP clash), which cannot be administered by all operating systemen (such as those from Microsoft). Therefore, one physical network segment has to be used for each firewall network interface.

The **Interfaces** menu allows you to configure and manage all network cards installed on the security system and also all interfaces with the external network (Internet) and interfaces to the internal networks (LAN, DMZ).

Note:

While planning your network topology and configuring the security system, take care to note which interface is connected to which network. In most configurations, the network interface with SysID **eth1** is chosen as the connection to the external network.

In order to install the **High Availability (HA)** system, the selected network cards on both systems must have the same SysID. Installing the **HA** system is described in more detail in chapter 5.1.10 on page 97.

The following sections explain how to use the **Current Interface Status** and **Hardware List** windows to manage the various **Interface types**.

Current Interface Status

Current Interface Status				
Admin	Oper	Name/Type	Parameters	Actions
	Up	Internal (Standard ethernet interface) on eth0	192.168.2.97 / 255.255.255.0 Gateway: 192.168.2.1	edit delete
Hardware List				
Sys ID	Name/Parameters			PCI Device ID
eth0	Realtek RT8139 irq=11 type=eth mac=00:10:dc:25:ac:80			
eth1	D-Link DFE-530TX rev A irq=9 type=eth mac=00:05:5d:a2:14:1b			
eth2	D-Link DFE-530TX rev A irq=5 type=eth mac=00:05:5d:a2:32:27			

This window allows you to configure both, logical and virtual **interfaces**. The table lists all interfaces which have already been configured.

The graphic at left shows the **Interfaces** menu after three Ethernet network cards have been configured.

During the installation, you will have configured the **eth0** interface. This interface is the connection between the security solution and the internal network (LAN). By default, this network card is named **Internal**. The table displays all of the most important information about the interfaces: the administrative status (enabled/disabled, indicated by a **green** or **red** status light), current connection status (**Up/Down**), Name (**Name**), ID (**Sys ID**), network card type (**eth/wlan**) as well as IP address and network mask (**Parameters**). Click the status light in the **Admin** column to administratively enable

Using the Security System

or disable the interface. The functions in the **Actions** column allow you to **edit** the configuration of the interface, or to **delete** it entirely.

With this Internet security system, you assign one **Name** and also a specific network card to one virtual interface. Three logical networks will then be defined for each configured interface:

- An interface (**NAME (Address)**), consisting of the defined IP address and the network mask 255.255.255.255 (Host)
- An interface (**NAME (Network)**), consisting of the defined IP address and the network mask 255.255.255.255 (Network)
- A Broadcast (**NAME (Broadcast)**) network, consisting of the broadcast IP for this interface and the network mask 255.255.255.255 (Host)

The networks are shown in the **Networks** menu. If an interface is configured using a dynamic addressing scheme, for example through **DHCP** or **PPPoE**, these settings are automatically updated. This means that all functions (for example, packet filter rules) configured with these aliases will automatically use the correct addresses.

Hardware List

Hardware List		
Sys ID	Name/Parameters	PCI Device ID
eth0	Realtek RTL8139 irq=11 type=eth mac=00:10:dc:25:ac:80	
eth1	D-Link DFE-530TX rev A irq=9 type=eth mac=00:05:5d:a2:14:1b	
eth2	D-Link DFE-530TX rev A irq=5 type=eth mac=00:05:5d:a2:32:27	

This table lists all network cards installed on the security system, together

with the relevant hardware information. The table shows, for example, the system-assigned ID (**Sys ID**), type of network card, hardware (MAC) address (**Name/Parameters**), and PCI bus information: Bus/Device/Function (**PCI Device ID**).

Error:

The **Hardware List** table doesn't list all of the network cards.

Possible Causes:



The missing network cards were added after the installation of the security system, or were not recognized during installation. Please contact the support department of your security system provider.

Attention:

If you change the **IP Address** of the internal network card (**eth0**), you may lock yourself out.

Using the Security System

5.3.2.1. Standard Ethernet Interface

To configure a network card for a standard Ethernet connection to an internal or external network, you must configure the card with an IP address and netmask.

All network cards installed on the security system are shown in the **Hardware List**.

Configuring a Standard Ethernet Connection:

1. In the **Network** tab, open the **Interfaces** menu.
2. Click on the **New** button.
The **Add Interface** window will open.
3. In the **Name** entry field, enter a descriptive name for the interface. (example: **Externally** for an Internet connection)
4. Use the **Hardware** drop-down menu to select a network card.

Tip:

For an external connection (e.g., to the Internet) choose the card with Sys ID **eth1**.

5. Use the drop-down menu **Type** to select **Standard Ethernet Interface**.

Please note that one network card cannot be used as both a **Standard ethernet interface** and a **PPP over Ethernet (PPPoE-DSL)** or **PPPTP over Ethernet (PPPoA-DSL) connection** simultaneously.

6. Now make the specific settings for this interface type:

Address: If you wish to use a static IP address for this interface, select **Static** from the drop-down menu and enter the address to use in the entry field. If you wish to have a gateway dynamically assigned via DHCP, select **Assign by DHCP** from the drop-down menu.

Netmask: If you wish to use a statically defined network mask for this interface, use the drop-down menu to select **Static** and enter the netmask to use in the entry field. If you wish to have a netmask dynamically assigned via DHCP, select **Assign by DHCP** from the drop-down menu.

Default Gateway: If you wish to use a statically defined default gateway, use the drop-down menu to select **Static** and enter the address of the gateway in the entry field. If you wish to have a gateway dynamically assigned via DHCP, select **Assign by DHCP** from the drop-down menu. Otherwise, select **None**.

Proxy ARP: When this function is enabled, the security system will answer ARP requests on the selected interface for all known networks. This system will thus act as a proxy on this interface for all of the other directly-connected networks.

This function is only required in special cases, for example when an attached network cannot be configured with normal routing entries (e.g., when the network includes a router over which you have no control).

By default, the **Proxy ARP** function is disabled (**Off**). To enable it, select **On** from the drop-down menu.

Uplink Failover on Interface: This function will only be displayed, if the parameter **Assign by DHCP** or **Static** has been selected in the **Default Gateway** drop-down menu.

If a network card is an interface to the Internet (e.g. 2 Megabit fixed connection) you can configure a standby connection by a second Internet access (e.g. DSL-connection) and an additional

Using the Security System

network card. If the primary connection fails, the uplink will automatically be set up through the second Internet access.

Note:

You need two separate Internet accesses and an additional network card for the **Uplink Failover on Interface** connection.

Uplink Failover on Interface is by default disabled (**Off**). If you wish to use this network card as primary Internet connection, then configure it in the **Primary Interface** drop-down menu. If this network card shall contain the standby connection, select the setting **Backup Interface**.

Uplink Failover check IP: Once the **Uplink Failover on Interface** function has been enabled, this entry field will be displayed. Enter the IP-address of a host that replies to ICMP-ping-requests (e.g., the DNS server of your ISP). The security system will send ping requests to this host: if no answer is received, the backup-interface will be enabled by the failover. In this entry field, there must always be an IP-address for the failover.

QoS Status: In order to use **Quality of Service (QoS)** bandwidth management on an interface, enable this option. To enable the **Quality of Service (QoS)** function, select **On** from the drop-down menu.

Important Note:

For the bandwidth management **Quality of Service (QoS)** you must define the values for **Uplink Bandwidth (kbits)** and **Downlink Bandwidth (kbits)**. These values are used as basis for the bandwidth management system: incorrect values can lead to poor management of the data flow. The **Quality of Service (QoS)** function is described in chapter 5.5.1.

Uplink Bandwidth (kbits): These settings will only appear, if the QoS function is enabled. In this entry menu, enter the

available bandwidth for the Uplink in full kilobits. This value can be determined either from the values of the upstream interface or from the router. On an interface to the Internet, this value corresponds to the bandwidth of the Internet connection - on an ADSL access the Uplink bandwidth amounts to 128 kBit/s and on a 2-Megabit fixed connection to 2048 kBit/s.

Downlink Bandwidth (kbits): These settings will only appear, if the QoS function is enabled. In this entry menu, enter the available bandwidth for the Downlink in full kilobits. On an interface to the Internet, this value corresponds to the bandwidth of the Internet connection - on an ADSL access the Uplink bandwidth amounts to 768 kBit/s and on a 2-Megabit fixed connection to 2048 kBit/s.

MTU Size: The **MTU** is the size (in bytes) of the largest transmittable packet. **MTU** stands for **Maximum Transfer Unit**. For connections, using the TCP/IP protocol, the data will be grouped into packets. A maximum size will be defined for these packets. Packets larger than this value will be considered too long for the connection and fragmented into smaller ones before transmission. These data packets will be sent again. However, the performance can be limited, if the upper value is too low. The largest possible MTU for an Ethernet interface is 1500 Bytes. The following values are the defaults for the **Standard Ethernet Interface**: 1500 Byte.

7. Confirm these settings by clicking **Add**.

The system will now check the address and netmask for semantic validity. After a successful check, the new **interface** will appear in the **Current Interface Status** table. The interface is not yet enabled (status light is red)

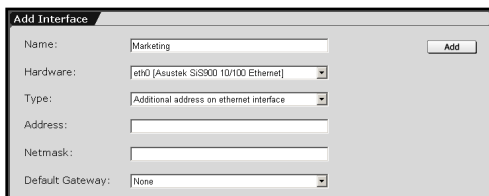
8. Enable the interface by clicking the status light.

The interface is now enabled (status light shows green). The **Oper** column will at first show that the interface is **Down**: the system

Using the Security System

requires a short time to configure and load the settings. When the message **Up** appears, the interface is fully operational.

5.3.2.2. Additional Address on Ethernet Interface



One network card can be configured with multiple additional IP addresses (also called IP aliases). This function allows you to manage multiple logical networks on

one physical network card. It can also be used to assign further addresses to a security system running **NAT**. **NAT** is described in further detail in chapter 5.3.4 on page 157. Each network card can be configured with up to 255 additional addresses.

Adding additional addresses to a network card:

1. In the **Network** tab, open the **Interfaces** menu.
2. Click on the **New** button.
The **Add Interface** window will open.
3. In the **Name** entry field, enter a descriptive name for the interface.
4. Use the **Hardware** drop-down menu to select a network card.
5. Use the **Type** drop-down menu to select **Additional address on Ethernet interface**.
6. Now make the specific settings for this interface type:

Address: For this interface type, the address must be statically defined. This kind of interface can only use static addresses.

Netmask: This interface type requires a statically defined netmask. This kind of interface can only use static masks.

Default Gateway: If you wish to use a default gateway with this interface, select **Static** from the drop-down menu and enter the gateway address in the entry field. Otherwise, select **None**.

7. Confirm these settings by clicking **Add**.

The system will now check the address and netmask for semantic validity. After a successful check, the new **interface** will appear in the **Current Interface Status** table. The interface is not yet enabled (status light is red)

8. Enable the interface by clicking the status light.

The interface is now enabled (status light shows green). The **Oper** column will at first show that the interface is **Down**: the system requires a short time to configure and load the settings. When the message **Up** appears, the interface is fully operational.

Using the Security System

5.3.2.3. Wireless LAN

The industry standards IEEE 802.11 apply to **Wireless LAN**. This Internet security system supports the **IEEE 802.11b** protocol. This standard uses radio signals in the **ISM** frequencies (in the 2.4 GHz band) to communicate between nodes. **ISM** stands for **Industrial Scientific and Medical**. The ISM frequencies have been specifically allocated for unlicensed communication by industrial, scientific, and medical organizations, and are thus available for cost-free private use. The IEEE 802.11b standard allows for a maximum bandwidth of 11 Mbit/s. When planning your network design, however, please note that bandwidth actually available will be smaller when the distances between nodes are large.

Important Note:

In order to configure a **Wireless LAN**, you will need a **PCMCIA card** with a **Prism2**, **Prism2,5**- or **Prism3**-compatible chipset. The hardware supported by the security system is listed in the **Hardware Compatibility List for Astaro Security Linux** available at <http://docs.astaro.org>.

The wireless LAN interface on the security system can be configured either as a **Wireless LAN Access Point** or a **Wireless LAN Station**.

The **Wireless LAN Access Point** mode connects wireless nodes with one another: its function is analogous to that of a hub in a traditional wired network. Wireless nodes can also communicate with the (wired) LAN through the security system.

In the **Wireless LAN Station** mode, the security system functions as a normal node on an existing wireless network. Only in this mode can the system acquire an IP address through DHCP.

Wireless LAN Security

The 802.11 standard includes the **WEP** standard for encrypting radio communications. WEP stands for **Wired Equivalent Privacy**. This encryption method is based on the RC4 cipher, and uses a secret

string to encrypt and decrypt messages. Activating WEP requires this secret key to be configured on all interfaces on the wireless network. All transmissions over the network are encrypted with this key at the sending station, and then decrypted at the receiving station. Without this key, the data cannot be decrypted.

This security system can also use **WEP** for **Authentication**. A computer attempting to connect to the network which is not configured with the correct key will be dropped at the access point.

The **Wireless LAN Access Point** mode also allows **stations** to be selectively granted access to the network on the basis of **MAC Address**. Normally, in the interest of flexibility, a wireless LAN will allow any new node onto the network as long as it is configured with the correct WEP settings. An administrator may choose, however, to control which nodes should have access: Such a filter can be configured to allow only certain nodes – for instance, the one identified by MAC address 00:04:76:26:65:4C – onto the network. When a new node attempts to join the network, the security system will check its MAC address: if the hardware address is in the list of allowed nodes, it will be permitted to join, otherwise the connection will be dropped.

This security solution supports two kinds of **MAC address filter**: **negative** and **positive**. A **negative filter** allows all hardware addresses except those on the list to join the network. In the access control you only define those network cards that should not be accessed by Wireless LAN.

A **positive filter**, on the other hand, first of all excludes all MAC addresses. In the access control you define explicitly those network cards that should can be accessed by Wireless LAN.

If at all possible, a positive filter should be used, which is by far safer.

The following settings are required to configure a wireless LAN PCMCIA card:

- **SSID**: An acronym for **Service Set Identifier**: this is essentially the name of the network. More than one wireless LAN can coexist

Using the Security System

in the same physical space provided that they have different names or use separate channels. The name of a network can be chosen freely: the only requirement is that it not contain any space characters.

If you are configuring a **Wireless LAN Station** interface to connect to an already-existing wireless network, this must be the name of that network. The name can be up to 32 characters long.

- **Channel:** This system must be manually configured with the radio channel to use. If other wireless networks are in the area, you should choose an unused channel for your network.

Please also note that only certain channels may be used in certain countries:

Country	Channel
USA & Canada	1 to 11
Europe (ETSI)	1 to 14
Japan	1 to 14

Country	Channel
Spain	10/11
France	1 to 13

- **WEP:** In order to use WEP encryption, you will need at least one WEP key - up to four can be used. You can choose between a 40 bit and 104 bit keys. A 40-bit key requires 5 hexadecimal numbers, while a 104-bit key requires 13 numbers. Please note that a hexadecimal number is two characters, each either a number (0-9) or a letter (A-F).

Example of a 40-bit key: 17:A5:6B:45:23

- **Access Mode** (only for Wireless LAN Access Point mode): If you wish to use the MAC address filter, you must compile a list of the MAC addresses which are explicitly allowed to connect to the network (positive filter), or which are explicitly not allowed to (negative filter).

How to determine the MAC address of a computer is described in the next section.

Determining the MAC address:

If you have not yet installed your network card, you can simply examine it to determine its MAC address: the unique MAC address is usually printed on the card itself.

If the wireless LAN is already being used and you wish to install a new MAC filter, you can use the following commands on the mobile nodes to determine the MAC address. If you are configuring a small wireless LAN, the mobile computers are MS Windows computers, and you have physical access to them, follow these steps:

1. Open the **Command Prompt**.
2. The **Command Prompt** can be found in the **Start** menu, under **Programs/Accessories/Command Prompt**.

3. Enter the following command at the prompt:

ipconfig -all

4. Press the **Enter** key.

The **Physical Address** row contains the MAC address, for example 00-04-76-26-65-4C.

5. Close the command prompt.

If you have a larger network, you can use the ping program under MS Windows to determine the MAC addresses of remote nodes:

1. Make sure that the remote computer whose MAC address you wish to check is turned on and connected to the network.
2. Open the **Command Prompt**.

The **Command Prompt** can be found in the **Start** menu, under **Programs/Accessories/Command Prompt**.

3. Ping the destination computer by using the following command:

ping IP Address (e.g. ping 192.168.2.15)

4. Press the **Enter** key.

Using the Security System

If the destination computer is reachable, you will receive the ping replies and some information about network latency.

5. Enter the following command:

arp -g

6. Press the **Enter** key.

Your computer's local ARP table will now be displayed. The **Physical Address** column of this table shows the MAC address for each known IP address.

In order to connect to a remote computer on the same subnet, the local computer addresses Ethernet frames to the remote computer's MAC address. In order to do this, it must first determine the remote hardware address by issuing an ARP request. When you issue the ping request, your local computer automatically determines the remote computer's MAC address and stores it in the local ARP table for future use.

If you wish to configure a **PCMCIA Card** for the **Wireless LAN** as an **Access Point**, complete the following steps. Configuration as a **Station** is described on page 137.

Configuring a Wireless LAN Access Point:

1. In the **Network** tab, open the **Interfaces** menu.
2. Click on the **New** button.
The **Add Interface** window will open.
3. In the **Name** entry field, enter a descriptive name for the interface.
4. Use the **Hardware** drop-down menu to select the **Wireless LAN** network card.
5. Use the **Type** drop-down menu to select the **Wireless LAN Access Point** interface type.

6. Fill in the required settings for the **Wireless LAN Access Point**.

Address: Assign an IP address for the access point. For this interface type, the address must be statically defined. Enter the address into this entry field.

Netmask: This interface type requires a statically defined netmask. Enter the network mask into this entry field.

Default Gateway: If you wish to use a default gateway with this interface, select **Static** from the drop-down menu and enter the gateway address in the entry field. Otherwise, select **None**.

SSID: Enter the network name for the wireless network here. Enter a string without space characters here. This should be a string up to 32 characters long.

Channel: Use the drop-down menu to select a frequency channel for the network.

Use WEP: If you wish to use WEP encryption on the wireless LAN, select **Yes** from the drop-down menu.



Security Note:

You should always use WEP encryption, as an unencrypted network presents a serious threat to network security.

If you select **No** from the drop-down menu, the WEP-specific configuration options will be ignored by the system.

WEP Authentication: If you wish to enable WEP authentication, select **Yes** from the drop-down menu. All nodes on the wireless network must be configured with the correct **WEP Key**.

Require WEP: If you do not wish to allow nodes not supporting WEP onto the wireless network, choose **Yes** here.

WEP Key: Enter the WEP key to use in the **WEP Key 0 through 3** entry fields. In order to use WEP encryption, you will need at least one WEP key - up to four can be used.

For a 40-bit key, enter a string with 5 hexadecimal digits separated by colons. In order to use a 104-bit key, enter a string

Using the Security System

of 13 hexadecimal digits separated by colons. The string must consist of hexadecimal digits. Please note that a hexadecimal number is two characters, each either a number (0-9) or a letter (A-F).

Example of a 40-bit key: 17:A5:6B:45:23

Default WEP Key: Use the drop-down menu to choose one of the defined **WEP Keys** 0-3 which should be used as the default key. This key will be used as the current key, which all the other nodes must use to access the wireless network.

Access Mode: Choose the filter mode for the wireless LAN. If all nodes should be allowed access (subject, of course, to WEP restrictions), select **All stations can get access**.

If you wish to configure a **positive filter** select **Stations in Allowed MAC addrs can get access**. To use a **negative filter**, choose **Stations in Denied MAC addrs can not get access**.

Allowed MAC addrs: If you have chosen to use a **positive filter**, enter the MAC addresses of nodes allowed to access the wireless network in the access control list.

The **access control list** function is identical to the **ordered list** and is described in chapter 4.3.4 on page 39.

Denied MAC addrs: If you have chosen to use a **negative filter**, enter the MAC addresses of nodes explicitly not allowed to access the network in the access control list.

The **access control list** function is identical to the **ordered list** and is described in chapter 4.3.4 on page 39.

7. Confirm these settings by clicking **Add**.

The system will now check the address and netmask for semantic validity. After a successful check, the new **interface** will appear in the **Current Interface Status** table. The interface is not yet enabled (status light is red)

8. Enable the interface by clicking the status light.

The interface is now enabled (status light shows green). The **Oper** column will at first show that the interface is **Down**: the system requires a short time to configure and load the settings. When the message **Up** appears, the interface is fully operational.

Configuring a Wireless LAN Station:

1. In the **Network** tab, open the **Interfaces** menu.
2. Click on the **New** button.
The **Add Interface** window will open.
3. In the **Name** entry field, enter a descriptive name for the interface.
4. Use the **Hardware** drop-down menu to select the **Wireless LAN** network card.
5. Use the **Type** drop-down menu to select the **Wireless LAN Station** interface type.
6. Fill in the required settings for the **Wireless LAN Station**.

Address: Assign an IP address for the station. If you wish to use a static IP address for this interface, select **Static** from the drop-down menu and enter the address to use in the entry field. If you wish to have a gateway dynamically assigned via DHCP, select **Assign by DHCP** from the drop-down menu.

Netmask: If you wish to use a statically defined network mask for this interface, use the drop-down menu to select **Static** and enter the netmask to use in the entry field. If you wish to have a netmask dynamically assigned via DHCP, select **Assign by DHCP** from the drop-down menu.

Default Gateway: If you wish to use a statically defined default gateway, use the drop-down menu to select **Static** and enter the address of the gateway in the entry field. If you wish to have a

Using the Security System

gateway dynamically assigned via DHCP, select **Assign by DHCP** from the drop-down menu. Otherwise, select **None**.

SSID: Enter the network name for the wireless network here. If you wish to establish a connection with an already existing Wireless LAN, you must enter the existing network name.

Use WEP: If you wish to use WEP encryption on the wireless LAN, select **Yes** from the drop-down menu.



Security Note:

You should always use WEP encryption, as an unencrypted network presents a serious threat to network security.

If you select **No** from the drop-down menu, the WEP-specific configuration options will be ignored by the system.

WEP Authentication: If you wish to enable WEP authentication, select **Yes** from the drop-down menu. All nodes on the wireless network must be configured with the correct **WEP Key**.

Require WEP: If you do not wish to allow nodes not supporting WEP onto the wireless network, choose **Yes** here.

WEP Key: Enter the WEP key to use in the **WEP Key 0 through 3** entry fields. In order to use WEP encryption, you will need at least one WEP key - up to four can be used.

For a 40-bit key, enter a string with 5 hexadecimal digits separated by colons. In order to use a 104-bit key, enter a string of 13 hexadecimal digits separated by colons. The string must consist of hexadecimal digits. Please note that a hexadecimal number is two characters, each either a number (0-9) or a letter (A-F).

Example of a 40-bit key: 17:A5:6B:45:23

Default WEP Key: Use the drop-down menu to choose one of the defined **WEP Keys** 0-3 which should be used as the default key. This key will be used as the current key, which all the other nodes must use to access the wireless network.

7. Confirm these settings by clicking **Add**.

The system will now check the address and netmask for semantic validity. After a successful check, the new **interface** will appear in the **Current Interface Status** table. The interface is not yet enabled (status light is red)

8. Enable the interface by clicking the status light.

The interface is now enabled (status light shows green). The **Oper** column will at first show that the interface is **Down**: the system requires a short time to configure and load the settings. When the message **Up** appears, the interface is fully operational.

Using the Security System

5.3.2.4. Virtual LAN

The screenshot shows a configuration window titled "Add Interface". It contains the following fields and values:

- Name: Man_10
- Hardware: eth1 [Realtek RT8139]
- Type: VLAN ethernet interface
- Address: Static
- Netmask: Static
- Default Gateway: None
- VLAN Tag: (empty)
- QoS Status: Off
- MTU Size: 1500

Virtual LAN (VLAN) technology allows a network to be segregated into multiple smaller network segments at the Ethernet level (layer 2). This can be useful, for instance, when security considerations require that certain clients only be allowed to communicate with certain

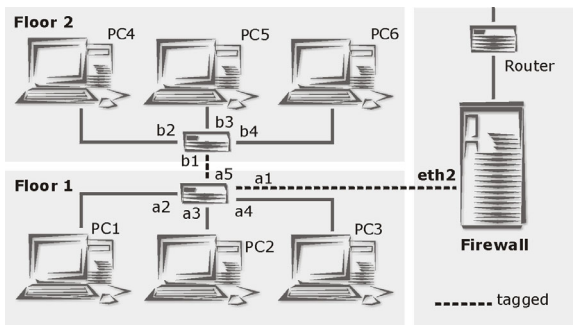
other ones. In large networks, this can also be useful to connect physically separate clients on the same logical network segment.

A VLAN-capable switch can assign ports to distinct groups. For example, a 20 port switch could assign ports 1 through 10 to VLAN 1, and ports 11 through 20 to VLAN 2. With such a configuration, a computer on port 1 would not be able to communicate with a computer on port 11. The technology essentially allows one physical switch to be divided into two logical ones.

In order to connect the security system to the virtual LANs, the system requires a network card with a **tag**-capable driver. A tag is a 4-byte header attached to packets as part of the Ethernet header. The tag contains the number of the VLAN that the packet should be sent to: the VLAN number is a 12-bit number, allowing up to 4095 virtual LANs. The WebAdmin tool refers to this number as the **VLAN Tag**.

The tagged packets are only used to communicate between the VLAN-compatible switch and the security system, the other computers on the network do not need to have tag-compatible network cards. The port on the switch connected to the security system must also be configured as an **untagged port**. Most VLAN-compatible switches can be configured by using a terminal program over a serial interface.

Example configuration:



The graphic at left shows an office where computers are distributed across two floors. Each floor has a separate switch, and the each computer is connected to the switch on its floor.

In this configuration, PC1 and PC2 on the first floor and PC4 on the second floor will be connected together on VLAN 10. PC3, PC5 and PC6 will be connected together on VLAN 20.

The two switches must be configured as follows:

Switch a

Port	VLAN Tag	tagged/ untagged
1	10, 20	T
2 (PC1)	10	U
3 (PC2)	10	U
4 (PC3)	20	U
5	10,20	T

Switch b

Port	VLAN Tag	tagged/ untagged
1	10, 20	T
2 (PC4)	10	U
3 (PC5)	20	U
4 (PC6)	20	U

In this configuration, it seems to PC3 as though it were connected through a single switch to PC5 and PC6.

In order to connect the computers to an external network (e.g., the Internet), the interface on the security system (in the example, this is eth2) must be configured to support the VLANs.

Attention:

In order to configure a **Virtual LAN** interface, you will need a network card with a **tag**-capable driver. The hardware supported by the security system is listed in the **Hardware Compatibility List for Astaro Security Linux** available at <http://docs.astaro.org>.

Configuring a Virtual LAN:

1. In the **Network** tab, open the **Interfaces** menu.
2. Click on the **New** button.
The **Add Interface** window will open.
3. In the **Name** entry field, enter a descriptive name for the interface.
4. Use the **Hardware** drop-down menu to select a network card.
5. Use the drop-down menu **Type** to select **VLAN Ethernet interface**.
6. Fill in the required settings for the **VLAN Ethernet Interface** type of interface:

Address: Assign an IP address for the virtual interface. If you wish to use a static IP address for this interface, select **Static** from the drop-down menu and enter the address to use in the entry field. If you wish to have a gateway dynamically assigned via DHCP, select **Assign by DHCP** from the drop-down menu.

Netmask: If you wish to use a statically defined network mask for this interface, use the drop-down menu to select **Static** and enter the netmask to use in the entry field. If you wish to have a netmask dynamically assigned via DHCP, select **Assign by DHCP** from the drop-down menu.

Default Gateway: If you wish to use a statically defined default gateway, use the drop-down menu to select **Static** and enter the address of the gateway in the entry field. If you wish to have a gateway dynamically assigned via DHCP, select **Assign by DHCP** from the drop-down menu. Otherwise, select **None**.

VLAN Tag: Enter the VLAN tag to use for this interface.

Uplink Failover on Interface this function will only be displayed if the **Assign by DHCP** or **Static** is selected in the **Default Gateway** drop-down menu.

You can configure a standby connection through a second interface. If the primary connection fails, the uplink will automatically be set-up through the second interface.

Uplink Failover on Interface is by default disabled (**Off**). If you wish to use this virtual interface as primary connection, select **Primary Interface** from the drop-down menu. If this interface shall contain the standby connection, select the **Backup Interface** configuration.

Uplink Failover check IP: Once the **Uplink Failover on Interface** function has been enabled, this entry field will be displayed. Enter the IP-address of a host that replies to ICMP-ping-requests. The security system will send ping requests to this host: if no answer is received, the backup-interface will be enabled by the failover. In this entry field, there must always be an IP-address for the failover.

QoS Status: In order to use **Quality of Service (QoS)** bandwidth management on an interface, enable this option. To enable the **Quality of Service (QoS)** module, select **On** from the drop-down menu.

Important Note:

For the bandwidth management **Quality of Service (QoS)** you must define the values for **Uplink Bandwidth (kbits)** and **Downlink Bandwidth (kbits)**. These values are used as basis for the bandwidth management system: incorrect values can lead to poor management of the data flow. The **Quality of Service (QoS)** function is described in chapter 5.5.1.

Uplink Bandwidth (kbits): These settings will only appear, if the QoS function is enabled. In this entry menu, enter the available bandwidth for the Uplink in full kilobits. This value can be determined either from the values of the upstream interface or from the router.

Downlink Bandwidth (kbits): These settings will only appear, if the QoS function is enabled. In this entry menu, enter the available bandwidth for the Downlink in full kilobits.

MTU Size: The **MTU** is the size (in bytes) of the largest transmittable packet. **MTU** stands for **Maximum Transfer Unit**. For connections, using the TCP/IP protocol, the data will be grouped into packets. A maximum size will be defined for these packets. Packets larger than this value will be considered too long for the connection and fragmented into smaller ones before transmission. These data packets will be sent again. However, the performance can be limited, if the upper value is too low.

The largest possible MTU for an Ethernet interface is 1500 Bytes. The following values are the defaults for the **VLAN Ethernet Interface**: 1500 Byte.

7. Confirm these settings by clicking **Add**.

The system will now check the address and netmask for semantic validity. After a successful check, the new **interface** will appear in the **Current Interface Status** table. The interface is not yet enabled (status light is red).

8. Enable the interface by clicking the status light.

The interface is now enabled (status light shows green). The **Oper** column will at first show that the interface is **Down**: the system requires a short time to configure and load the settings. When the message **Up** appears, the interface is fully operational.

The new virtual interface will appear in the **Hardware Device Overview** just as an additional IP address (IP alias) on a standard Ethernet network card would. The **Sys ID** of this virtual interface is composed of the SysID of the network card and the number of the VLAN tag.

5.3.2.5. PPPoE-DSL Connection

This interface type is used to connect to the Internet over a **DSL** connection using the **PPP over Ethernet** protocol. The configuration will require the DSL connection information, including username and password, provided by your Internet Service Provider.

Note:

The installation and specific settings required for **DSL** connections is described in the **DSL Network** guidebook. Also note that, once the DSL connection is activated, the security system will be connected to your ISP 24 hours a day. You should therefore ensure that your ISP bills on a flat-rate or bandwidth-based system rather than based on connection time. The **DSL Network** guidebook is available at <http://docs.astaro.org>.

Using the Security System

Configuring PPP over Ethernet (PPPoE-DSL):

1. In the **Network** tab, open the **Interfaces** menu.
2. Click on the **New** button.
The **Add Interface** window will open.
3. In the **Name** entry field, enter a descriptive name for the interface.
4. Use the **Hardware** drop-down menu to select a network card.

Tip:

For an external connection (e.g., to the Internet) choose the card with Sys ID **eth1**.

You cannot choose a network card that has already been configured with a primary network address.

5. Use the **Type** drop-down menu to select the **PPP over Ethernet (PPPoE-DSL) connection** interface type.

You will need the connection settings provided by your ISP to configure the following settings.

Address: If you have not been assigned a static IP address by your provider, keep the default **Assigned by remote** setting here. If you have a static IP address, choose **Static** from the drop-down menu and enter the address in the entry field.

Default Gateway: You should probably keep the default setting **Assigned by remote**. Other possible values are **Static** and **None**.

Username: Enter the username, provided by your ISP.

Password: Enter the password, provided by your ISP.

Uplink Failover on Interface this function will only be displayed if the **Assign by DHCP** or **Static** is selected in the **Default Gateway** drop-down menu.

You can configure a standby connection through a second interface. If the primary connection fails, the uplink will automatically be set-up through the second interface.

Note:

You need two separate Internet accesses and one additional network card for the **Uplink Failover on Interface** function. Please, note that the Security system only supports one DSL-connection. A standby connection for accessing the Internet can therefore only consist, for example, of a fixed connection and a DSL access.

Uplink Failover on Interface is by default disabled (**Off**). If you wish to use this virtual interface as primary connection, select **Primary Interface** from the drop-down menu. If this interface shall contain the standby connection, select the **Backup Interface** configuration.

Uplink Failover check IP: Once the **Uplink Failover on Interface** function has been enabled, this entry field will be displayed. Enter the IP-address of a host that replies to ICMP-ping-requests (e.g., the DNS server of your ISP). The security system will send ping requests to this host: if no answer is received, the backup-interface will be enabled by the failover. In this entry field, there must always be an IP-address for the failover.

QoS Status: In order to use **Quality of Service (QoS)** bandwidth management on an interface, enable this option. To enable the **Quality of Service (QoS)** module, select **On** from the drop-down menu.

Important Note:

For the bandwidth management **Quality of Service (QoS)** you must define the values for **Uplink Bandwidth (kbits)** and **Downlink Bandwidth (kbits)**. These values are used as basis for the bandwidth management system: incorrect values can lead to poor management of the data flow. The **Quality of Service (QoS)** function is described in chapter 5.5.1.

Uplink Bandwidth (kbits): These settings will only appear, if the QoS function is enabled. In this entry menu, enter the available bandwidth for the Uplink in full kilobits. This value can be determined either from the values of the upstream interface or from the router. On an interface to the Internet, this value corresponds to the bandwidth of the Internet connection - on an ADSL access the Uplink bandwidth amounts to 128 kBit/s and on a 2-Megabit fixed connection to 2048 kBit/s.

Downlink Bandwidth (kbits): These settings will only appear, if the QoS function is enabled. In this entry menu, enter the available bandwidth for the Downlink in full kilobits. On an interface to the Internet, this value corresponds to the bandwidth of the Internet connection - on an ADSL access the Uplink bandwidth amounts to 768 kBit/s and on a 2-Megabit fixed connection to 2048 kBit/s.

MTU Size: The **MTU** is the size (in bytes) of the largest transmittable packet. **MTU** stands for **Maximum Transfer Unit**. For connections, using the TCP/IP protocol, the data will be subdivided into packets. A maximum size will be defined for these packets. Packets larger than this value will be considered too long for the connection and fragmented into smaller ones before transmission. These data packets will be sent again. However, the performance can be limited, if the upper value is too low.

Using the Security System

The following values are the defaults for the **PPP over Ethernet (PPPoE-DSL) connection: 1492** Byte.

6. Confirm these settings by clicking **Add**.

The system will now check the address and netmask for semantic validity. After a successful check, the new **interface** will appear in the **Current Interface Status** table. The interface is not yet enabled (status light is red).

7. Enable the interface by clicking the status light.

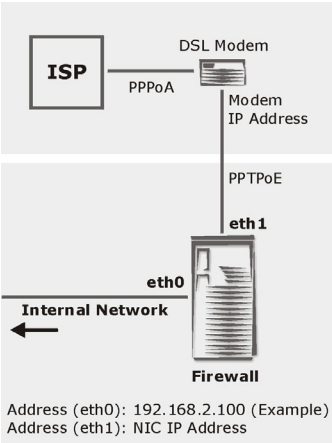
The interface is now enabled (status light shows green). The **Oper** column will at first show that the interface is **Down**: the system requires a short time to configure and load the settings. When the message **Up** appears, the interface is fully operational.

Using the Security System

5.3.2.6. PPTPoE/PPPoA-DSL Connections

Name:	dsl	<input type="button" value="Add"/>
Hardware:	eth1 [Realtek RTB139]	
Type:	PPTP over Ethernet (PPPoA-DSL) connection	
Address:	Assigned by remote	
Default Gateway:	Assigned by remote	
Modem IP Address:	<input type="text"/>	
NIC IP Address:	<input type="text"/>	
NIC Netmask:	<input type="text"/>	
Address to Ping:	<input type="text"/>	
Username:	<input type="text"/>	
Password:	<input type="text"/>	
Uplink Failover on Interface:	Off	
QoS Status:	Off	
MTU Size:	1460	

This type of interface is required for **DSL** connections using the **PPP over ATM** protocol. To configure such a connection, you will need an unused Ethernet interface on the security system as well as an ADSL modem with an Ethernet port. The connection to the Internet proceeds through two separate con-



nections (see graphic): Between the security system and the ADSL modem, a connection using the **PPTP over Ethernet** protocol is established. The ADSL modem is, in turn, connected to the ISP using the **PPP over ATM** dialing protocol.

The configuration will require the DSL connection information, including user-name and password, provided by your Internet Service Provider.

Note:

The installation and specific settings required for **DSL** connections is described in the **DSL Network** guidebook. Also note that, once the DSL connection is activated, the security system will be connected to your ISP 24 hours a day. You should therefore ensure that your ISP bills on a flat-rate or bandwidth-based system rather than based on connection time. The **DSL Network** guidebook is available at <http://docs.astaro.org>.

Configuring PPTP over Ethernet (PPPoA-DSL):

1. In the **Network** tab, open the **Interfaces** menu.
2. Click the **New** button to open the **Add Interface** window.
3. In the **Name** entry field, enter a descriptive name for the interface.
4. Use the **Hardware** drop-down menu to select a network card.

Tip:

For an external connection (e.g., to the Internet) choose the card with Sys ID **eth1**.

You cannot choose a network card that has already been configured with a primary network address.

5. Use the **Type** drop-down menu to select the **PPTP over Ethernet (PPPoA-DSL) connection** interface type.

You will need the connection settings provided by your ISP to configure the following settings.

Address: If you have not been assigned a static IP address by your provider, keep the default **Assigned by remote** setting here.

Using the Security System

If you have a static IP address, choose **Static** from the drop-down menu and enter the address in the entry field.

Default Gateway: You should probably keep the default setting **Assigned by remote**. Other possible values are **Static** and **None**.

Modem IP Address: Enter the IP address of your ADSL modem here. This address will usually be provided by your ISP or the modem hardware, and cannot be changed.

Example: 10.0.0.138 (with **AonSpeed**)

NIC IP Address: Enter the IP address of the network card on the security system which is attached to the modem here. This address must be in the same subnet as the modem.

Example: 10.0.0.140 (with **AonSpeed**)

NIC Netmask: Enter the network mask to use here.

Example: 255.255.255.0 (with **AonSpeed**)

Address to Ping: In order to test the connection between the security system and the external network, you can enter an IP address of a host on the Internet (e.g., the DNS server of your ISP) here. The security system will send ping requests to this host: if no answer is received, the connection will be broken.

Username: Enter the username, provided by your ISP.

Password: Enter the password, provided by your ISP.

Click **Enable** to open the **Advanced options** configuration settings.

Uplink Failover on Interface this function will only be displayed if the **Assign by DHCP** or **Static** is selected in the **Default Gateway** drop-down menu.

You can configure a standby connection through a second interface. If the primary connection fails, the uplink will automatically be set-up through the second interface.

Note:

You need two separate Internet accesses and one additional network card for the **Uplink Failover on Interface** function. Please, note that the Security system only supports one DSL-connection. A standby connection for accessing the Internet can therefore only consist, for example, of a fixed connection and a DSL access.

Uplink Failover on Interface is by default disabled (**Off**). If you wish to use this virtual interface as primary connection, select **Primary Interface** from the drop-down menu. If this interface shall contain the standby connection, select the **Backup Interface** configuration.

Uplink Failover check IP: Once the **Uplink Failover on Interface** function has been enabled, this entry field will be displayed. Enter the IP-address of a host that replies to ICMP-ping-requests (e.g., the DNS server of your ISP). The security system will send ping requests to this host: if no answer is received, the backup-interface will be enabled by the failover. In this entry field, there must always be an IP-address for the failover.

QoS Status: In order to use **Quality of Service (QoS)** bandwidth management on an interface, enable this option. To enable the **Quality of Service (QoS)** module, select **On** from the drop-down menu.

Important Note:

For the bandwidth management **Quality of Service (QoS)** you must define the values for **Uplink Bandwidth (kbits)** and **Downlink Bandwidth (kbits)**. These values are used as basis for the bandwidth management system: incorrect values can lead to poor management of the data flow. The **Quality of Service (QoS)** function is described in chapter 5.5.1.

Using the Security System

Uplink Bandwidth (kbits): These settings will only appear, if the QoS function is enabled. In this entry menu, enter the available bandwidth for the Uplink in full kilobits. This value can be determined either from the values of the upstream interface or from the router. On an interface to the Internet, this value corresponds to the bandwidth of the Internet connection - on an ADSL access the Uplink bandwidth amounts to 128 kBit/s and on a 2-Megabit fixed connection to 2048 kBit/s.

Downlink Bandwidth (kbits): These settings will only appear, if the QoS function is enabled. In this entry menu, enter the available bandwidth for the Downlink in full kilobits. On an interface to the Internet, this value corresponds to the bandwidth of the Internet connection - on an ADSL access the Uplink bandwidth amounts to 768 kBit/s and on a 2-Megabit fixed connection to 2048 kBit/s.

MTU Size: The **MTU** is the size (in bytes) of the largest transmittable packet. **MTU** stands for **Maximum Transfer Unit**. For connections, using the TCP/IP protocol, the data will be subdivided into packets. A maximum size will be defined for these packets. Packets larger than this value will be considered too long for the connection and fragmented into smaller ones before transmission. These data packets will be sent again. However, the performance can be limited, if the upper value is too low.

The following values are the defaults for the **PPP over Ethernet (PPPoA-DSL) connection: 1460** Byte.

6. Confirm these settings by clicking **Add**.

The system will now check the address and netmask for semantic validity. After a successful check, the new **interface** will appear in the **Current Interface Status** table. The interface is not yet enabled (status light is red)

7. Enable the interface by clicking the status light.

The screenshot shows a web-based configuration interface. The top section is titled 'Add Static Route' and contains two dropdown menus labeled 'Network:' and 'Target:', both with the text 'Please select :'. To the right of these is a 'Save' button. Below this is a section titled 'Static Routes' which contains a table with three columns: 'Network', 'Target', and 'Actions'. The table is currently empty, with the text ': no additional static routes defined :'. Below the 'Static Routes' section is a section titled 'Kernel Routing Table' which contains a 'View raw Kernel Routing Table:' label and a 'Show' button.

The interface is now enabled (status light shows green). The **Oper** column will at first show that the interface is **Down**: the system requires a short time to con-

figure and load the settings. When the message **Up** appears, the interface is fully operational.

5.3.3. Routing

Every network-connected computer uses a routing table to determine where outbound packets should be sent. The routing table contains the information necessary to determine, for instance, if the destination address is on the local network, or if traffic must be sent via a router – and, if a router is to be used, the table details which router is to be used for which network.

Static Routes

The security system will install static routing entries for directly-connected networks by itself. Further routes, however, must be manually entered. This is the case, for instance, when the local network includes a router to be used for access to a specific network. These routes, called static routes, contain information about how to contact a non-directly connected network.

This menu allows you to define which network card or router should be used to contact various external networks.

Using the Security System

Defining Static Routes:

1. Under the **Network** tab, open the **Routing** menu.

2. Click on the **New** button.

The **Add Static Route** window will open.

3. In the **Network** drop-down menu, choose the network you wish to define a route for.

The **Network** drop-down menu contains all static networks, as well as those you have defined in the **Networks** and **Interfaces** menus.

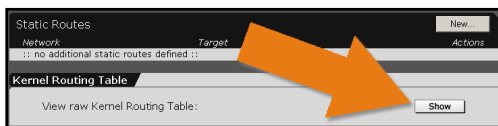
4. In the **Target** drop-down menu, select the destination to which packets should be forwarded.

Names in brackets are **interfaces**, while names without are hosts or routers. Names without brackets are either hosts or routers.

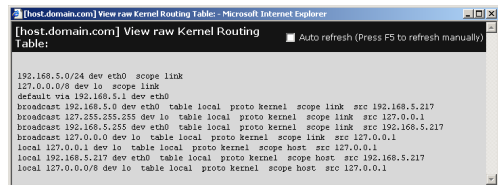
5. Save your changes by clicking **Save**.

When a new route has been defined and saved, it will appear in the **Static Routes** table. To remove an entry, click **delete**.

Kernel Routing Table



The **Kernel Routing Table** will be displayed in a separate window. This window



shows all on the system currently active routes. The system will check each rule in the order of the list, using the first applicable route. By default, the default routes

associated with network cards are already entered, and are not editable.

Clicking on the **Show** button opens the *Kernel Routing Table* window.

5.3.4. NAT/Masquerading

5.3.4.1. NAT

Add New NAT Rule					
Name:		nat		Add	
Rule Type:		DNAT/SNAT			
Packets to match:					
Source address		Destination address		Service	
: No match :		: No match :		: No match :	
Change Source to:		Address			
		: No change :			
Change Destination to:		Address			
		: No change :			
NAT Rules					
State	Name	Match Parameters	SRC Translation	DST Translation	Actions
:: No NAT rules defined ::					

The **Network Address Translation (NAT)** function translates one set of IP addresses (usually private ones) to addresses in another set (usually public). NAT makes it possible for computers on an internal LAN to use private IP addresses, while still allowing

them to communicate – through the security system – with the public Internet.

When a client sends an IP packet to the router, NAT translates the sending address to a different, public IP address (from the address space given by the Internet provider) before forwarding the packet to the Internet. When a response packet is received, NAT translates the public address into the original address and forwards it on to the internal client. Depending on system resources, the NAT function can handle arbitrarily large internal networks.

Destination Network Address Translation (DNAT) is a special case of NAT whereby the destination addresses of packets are translated. This is especially useful when an internal network uses private IP addresses, but an administrator wishes to make some services available to the public Internet.

Using the Security System

Important Note:

PPTP VPN Access is incompatible with **DNAT**.

Example:

Your internal network uses the address space 192.168.0.0/255.255.255.0 and a web server running at IP address 192.168.0.20 port 80 should be available to Internet-based clients.

Because the 192.168 address space is private, the Internet-based clients cannot send packets directly to the web server. It is, however, possible for them to communicate with the external (public) address of the security system. **DNAT** can, in this case, take packets addressed to port 80 of the system's address and forward them to the internal web server.

Note:

The method of setting up a **web server** behind the Internet security solution is described in the **Web Server/DNAT** guidebook. The **Web Server/DNAT** guidebook is available at <http://docs.astaro.org>.

Source Network Address Translation (SNAT) is another special case of **NAT**, and functions just as **DNAT** does, with the difference that **source addresses** (rather than **destination addresses**) are translated.

This is useful in complex networks where replies should be sent from other network addresses.

Tip:

To build a simple translation system from an internal network to the Internet, use the **Masquerading** function instead of **SNAT**.

In contrast to **Masquerading**, which is dynamic, **SNAT** uses a static address translation. That is, every internal address is translated to its own externally visible **IP address**.

Note:

In order to forward port 443 (HTTPS) to an internal server, you must first change the value of the **WebAdmin TCP Port** (e.g., 1443) for WebAdmin in the **System/WebAdmin Settings** menu. This function is described in chapter 5.1.8 in chapter **General Settings**.

Note:

Because translation occurs before **Packet filtering**, you must ensure that appropriate rules are entered in the **Packet Filter/Rules** menu. More information on setting packet filter rules can be found in chapter 5.4 on page 179.

Defining NAT rules:

1. In the **Network** tab, open the **NAT/Masquerading** menu.
2. In the **Name** field, enter a descriptive name for this **NAT** rule.
3. In the **Rule type** drop-down menu, select the **DNAT/SNAT** function.

A window named **Properties** will open.

4. In the **Packets to match** window, define which packets should be translated.

At least one parameter in this window must be defined in order to create a valid DNAT/SNAT rule. The setting **No match** means that packets will not be matched on the basis of this parameter.

Using the Security System

Source address: Choose the original source address here: This can be either a single host or an entire network.

Destination address: Choose the original destination address here: This can be either a single host or an entire network.

Service: Choose the original service here: the service is defined by source and destination ports as well as protocol used (e.g., TCP).

Note:

A **service** can only be redirected when the communicating addresses are also redirected. In addition, a service can only be redirected to another service when the two services use the same protocol.

5. Use the next drop-down menus to define how the packets should be translated.

At least one parameter in this window must be defined in order to create a valid DNAT/SNAT rule. If you redirect the original address to an entire network, the addresses in that network will be used one after another.

Change Source to (SNAT): Choose a new source address for the translated packets. This can be either a single host or an entire network.

Service source: This drop-down menu will only be shown when you have chosen an address in the **Change source to** menu. Only services with one source port can be used here.

Change Destination to (DNAT): Choose a new destination address here. This can be either a single host or an entire network.

Service destination: This drop-down menu will only be shown when you have chosen an address in the **Change destination to** menu.

6. Save the settings by clicking **Add**.

After successfully defining a rule, it will appear in the **NAT Rules** table list. The further functions in the NAT table can now be used for further customization.

Further Functions

Edit rule: Click **edit** to load the rule into the **Edit NAT Rule** window. The rule can now be changed as desired.

Delete rule: Click **Delete** to remove a rule from the list.

5.3.4.2. Masquerading

Masquerading is a special case of **SNAT**, which allows you to associate many internal (private) addresses with one external (public) address. This allows you to hide

internal IP addresses and network information from the outside network.

The differences between Masquerading and SNAT are:

- Masquerading requires a source network. It will automatically include all services (ports) on that network.
- The translation only occurs when the packet is sent via the supplied network card. The new source address will be that of the interface.

Masquerading is intended to hide privately addressed LANs behind one official (public) Internet address.

Using the Security System

Defining Masquerading rules:

To define masquerading rules, select which network should masquerade as which network card. Normally, the external network card is used.

Note:

In order for clients from the defined network to build a connection to the Internet, the appropriate rules must be entered in the **Packet Filter/Rules** menu.

More information on setting packet filter rules can be found in chapter 5.4 on page 179.

1. In the **Network** tab, open the **NAT/Masquerading** menu.
2. In the **Name** field, enter a descriptive name for this **Masquerading Rule**.
3. Use the **Rule type** drop-down menu to select **Masquerading**.
A window named **Properties** will open.
4. Use the **Network** drop-down menu to select a network.
5. Use the **Interface** drop-down menu to select an interface.
6. Save the settings by clicking **Add**.

After a *masquerading rule* has been defined and added, it will appear in the **NAT rules** table. The further functions in the NAT table can now be used for further customization.

Further Functions

Edit Masquerading rules: Click **edit** to load the rule into the **Edit NAT Rule** window. The rule can now be changed as desired.

Deleting Masquerading rules: Click **delete** to remove a rule from the list.

5.3.4.3. Load Balancing

The **Load Balancing** function allows you to balance incoming connections (e.g. SMTP or HTTP sessions) across different servers behind the security system.

Example: In the enterprise's DMZ sit two identical HTTP servers with

IP addresses 192.168.66.10 and 192.168.66.20. *Load Balancing* can split incoming HTTP requests between the two servers evenly.

Before the load-balancing rule can be defined, the two HTTP servers must be defined as networks (consisting of single hosts) in the **Definitions/Networks** menu. Next, add both to a single network group.

The procedures for adding **networks** and **network groups** are described in chapters 5.2.1 and 103, respectively.

Once these definitions have been saved, the *load balancing* rules can be defined.

Defining Load Balancing rules:

1. In the **Network** tab, open the **NAT/Masquerading** menu.
2. Enter a descriptive name for the **load-balancing rule** in the **Name** entry field.

A window named **Properties** will open.

3. Enter a descriptive name for the **load-balancing rule** in the **Name** entry field.
4. Use the **Rule Type** drop-down menu to select **Load Balancing**.

Using the Security System

5. In the **Pre-Balancing Target** window, select the original destination address and service.

Address or Hostname: Select the original destination address here. This should usually be the external address of the security system.

Service: Select the destination port (service) to be balanced.

6. In the **Post-Balancing Target Group** drop-down menu, select the new address. This will usually be a network group composed of single hosts.

When the load-balancing rule has been defined and saved, it will appear in the **NAT rules** table. The further functions in the NAT table can now be used for further customization.

Editing Load Balancing rules: Click **edit** to load the rule into the **Edit NAT Rule** window. The rule can now be changed as desired.

Deleting Load Balancing rules: Click **delete** to remove a rule from the list.

5.3.5. DHCP Server

DHCP Server

Select Interface: Internal

Status: ☒ Disable

Range Start: 192.168.5.1 Save

Range End: 192.168.5.254

DNS Server 1 IP:

DNS Server 2 IP:

Gateway IP:

WINS Server IP:

WINS Node Type: B-Node Broadcast - no WINS

Static Mappings

MAC Address	IP Address	Comment
<input type="text"/> <input type="text"/> <input type="text"/> Add		

Static Mapping Table

MAC Address	IP Address	Comment	Actions
no mappings defined			

The **Dynamic Host Configuration Protocol (DHCP)** automatically distributes addresses from a defined IP address pool to client computers. It is designed to simplify network configuration on large networks, and to prevent address conflicts. DHCP distributes IP addresses, default gateway information, and DNS configuration information to its clients.

In addition to simplifying the configuration of client computers and allowing mobile computers to move painlessly between networks, DHCP helps to localize and troubleshoot IP address-related problems, as these are mostly issues with the configuration of the DHCP server itself. It also allows for a more effective use of address space, especially when not all computers will be active at the same time. as addresses can be distributed as needed and re-used when unneeded.

Configuring the DHCP Server:

1. In the **Network** tab, open the **DHCP Server** menu.
2. In the **Interface** drop-down menu, select the interface from which the IP addresses should be assigned to the clients.
3. Click **Enable** next to **Status** to enable the function.
Another entry window will open.
4. Use the **Range Start** and **Range End** menus to set the address space from which IP addresses will be distributed.

Using the Security System

By default, the configured address area of the network card will appear in the entry field.

The settings will take effect without further confirmation.

Assigning DNS Servers and Gateway IP Addresses:

You can transmit further parameters for the network configuration to the clients. Such as the DNS Server Addresses and the Default Gateway to be used by the clients. The security system itself will usually fill both of these functions: in this case, you should enter the internal address of the system in these entry fields.

The DNS Proxy is configured in the **Proxies/DNS** menu. Please see chapter 5.6.2 on page 227 for a description of how to use the DNS proxy.

NetBIOS networks can also use a **WINS** server for name resolution. WINS stands for Windows Internet Name Service. WINS servers are MS Windows NT servers with both the Microsoft TCP/IP stack and the WINS server software installed. These servers act as a database matching computer names with IP addresses, thus allowing computers using NetBIOS networking to take advantage of the TCP/IP network.

1. In the **Network** tab, open the **DHCP Server** menu.
2. In the entry fields **DNS Server 1 IP** and **DNS Server 2 IP**, enter the IP address of your name servers.
3. In the **Gateway IP** entry field, enter the IP address of the default gateway.
4. If you wish to assign a **WINS** server, configure the following two settings:

WINS Server IP: Enter the IP address of the WINS server here.

WINS Node Type: Use the drop-down menu to choose which kind of name resolution clients should use. If you choose **Do not set node type**, the client will choose by itself which to use.

5. Save your configuration by clicking **Save**.

Configuring Static Mappings:

This function allows you to ensure that specific computers are always assigned the same IP address. To configure this function, you will need to know the MAC (hardware) address of the client's network card.

Determining the MAC addresses of network cards is described on page 133.

1. In the **Network** tab, open the **DHCP Server** menu.
2. In the **Static Mappings** window, make the following settings:
 - MAC Address:** In the MAC Address entry field, enter the MAC address of the network card. The MAC address must be entered as in the following example
Example: 00:04:76:16:EA:62
 - IP Address:** Enter the IP address into this entry field. The address must be within the range specified by the **Range Start** and **Range End** options.
3. Save the settings by clicking **Add**.

The static address mapping will appear in the **Static Mapping Table**. To remove an entry from this table, click **delete**.

Using the Security System

Current IP Leasing Table

The **Current IP Leasing** table shows all current IP address mappings. If more than one entry is shown for the same IP address, only the last-listed one is valid. This table will only be shown when there are entries in it.

5.3.6. PPTP VPN

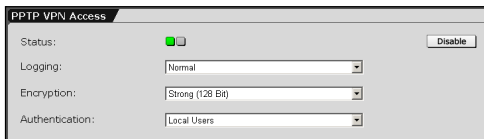
Point-to-Point Tunneling Protocol (PPTP) allows single Internet-based hosts to access internal network services through an encrypted tunnel. **PPTP** is easy to set-up, and requires on Microsoft Windows systems no special client software.

PPTP is included with versions of Microsoft Windows starting with Windows 95. In order to use **PPTP** with this security system, the client computer must support the MSCHAPv2 authentication protocol. Windows 95 and 98 users must apply an update to their systems in order to support this protocol. The update is available from Microsoft at:

<http://support.microsoft.com/support/kb/articles/Q191/5/40.ASP>

Select the VPN Update and, if you use Windows 95, also the RAS Update.

PPTP VPN Access



This window allows you to enable or disable **PPTP VPN** access by clicking the **Enable/Disable** button.

Logging: This drop-down menu allows you to choose how detailed the information recorded in the **PPTP Logs** should be. The **Extensive** setting should be used when you are using the **Live Log** to debug connection problems. When you start the connection, you can view the process in real time.

The **PPTP Live Log** is in the **Local Logs/Browse** menu.

Encryption: This drop-down menu allows you to choose between encryption strengths (40-bit or 128-bit). Note that, in contrast to Windows 98 and Windows ME, Windows 2000 does not come with 128 bit encryption installed: to use this kind of connection, the **High**

Using the Security System

Encryption Pack or **Service Pack 2** must be installed. **SP2** cannot be uninstalled later.



Security Note:

You should always set **Encryption** to **Strong** (128-bit) except when your network includes endpoints, which cannot support this.

Authentication: Use this drop-down menu to select an authentication method. If you have defined a RADIUS server in the **System/User Authentication** menu, you can use RADIUS authentication here as well.

The configuration of the Microsoft IAS RADIUS server and the configuration of RADIUS within **WebAdmin** is described in chapter 5.1.7 on page 71.

The **PPTP Live Log** provides a list of important events, including error messages, related to the PPTP service. The **Logging** menu can be used to select which events are logged.

PPTP IP Pool

The screenshot shows a window titled "PPTP VPN Access". It contains four configuration rows: "Status:" with a checked checkbox and a "Disable" button; "Logging:" with a dropdown menu set to "Normal"; "Encryption:" with a dropdown menu set to "Strong (128 Bit)"; and "Authentication:" with a dropdown menu set to "Local Users".

This menu is used to define which IP addresses PPTP hosts should be assigned. The default settings assign addresses from the private

IP space 10.x.x.x. This network is called the **PPTP Pool**, and can be used in all of the other security system configuration options. If you wish to use a different network, simply change the definition of the *PPTP Pool*, or assign another defined network as *PPTP Pool* here.

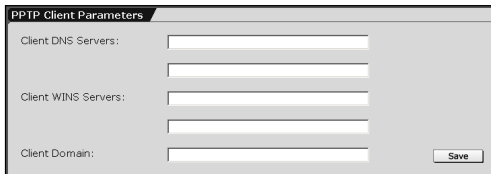
PPTP users are defined in the **Definitions/Users** menu. It is also possible to assign specific users to specific IP addresses. These addresses do not need to be part of the defined PPTP pool. To use

these addresses in other parts of the system configuration, such as the packet filter, they must be defined as single hosts (i.e., networks with netmask 255.255.255.255) or as a part of a larger network.

Note:

If you use private IP addresses for the **PPTP pool** and you wish *PPTP*-connected computers to be allowed to access the Internet, appropriate **Masquerading** or **NAT** rules must be in place.

PPTP Client Parameters



This window allows you to define name servers (DNS and WINS) and the name service domain, which should be assigned to hosts during the connection establishment.

Connections with MS Windows 2000:

The following example shows how to configure a PPTP VPN connection on a Windows 2000 host.

1. Under the **Network** tab, open the **PPTP VPN Access** menu.
2. In the **PPTP VPN Access** window, enable the system by clicking **Enable**.

The status light will show green and the menu will open.

3. In the **PPTP VPN Access** window, make the settings for the network access:

Logging: Keep the setting **Normal**.

Using the Security System

Encryption: In the drop-down menu, select the encryption type. The available options are **weak (40 bit)** and **strong (128 bit)**. Note that, in contrast to Windows 98 and Windows ME, Windows 2000 does not come with 128 bit encryption installed: to use this kind of connection, the **High Encryption Pack** or **Service Pack 2** must be installed. **SP2** cannot be uninstalled later. The selected encryption strength will take effect immediately.

Important Note:

Both sides of the connection must use the same encryption strength. If **WebAdmin** is set to use 40-bit encryption, and the MS Windows 2000 client is set to use 128-bit encryption, Windows will incorrectly report that the connection has been established.

Authentication: Use the drop-down menu to select a service.

4. Now define which IP addresses should be assigned to the hosts when connecting. In the **PPTP IP Pool** window, use the **Network** drop-down menu to select a network. The chosen network will be used immediately.

The **PPTP Pool** network is selected by default.

The IP address, network mask, and number of free addresses will appear below the drop-down box.

Users will be assigned an address from this range automatically.

5. In the **PPTP Client Parameters** window, DNS and WINS servers for PPTP clients can be defined. Two servers may be defined for each.

Client DNS servers: Enter the IP addresses of the DNS servers to use.

Client WINS Servers: Enter the IP addresses of the Windows name servers to use.

Client domain: Enter the DNS domain that the client should append to DNS requests.

6. Save your configuration by clicking **Save**.

The rest of the configuration takes place on the user's machine. This will require the IP address of the server, as well as a valid username and password. These should be supplied by the security system administrator.

1. In Microsoft Windows 2000, open the **Start/Settings/Network and Dialup Connections** menu.

2. Click the **Make New Connection** icon.

The **Network Connection Wizard** will open.

Then click on the **Next** button.

3. Select the following option: **Connect to a private network through the Internet**.

Then click on the **Next** button.

4. If you have a permanent connection to the Internet, select the following option **Do not dial the initial connection**.

Then click on the **Next** button.

Otherwise, select the **Dial other connections first option** and select your provider from the selection menu. These settings can be changed later in the **Properties** dialog box.

5. In the **Destination address** entry field, enter the IP address of the server.

Then click on the **Next** button.

6. In the **Connection Availability** window, select whether the connection should be available to all local users, or just this account.

Then click on the **Next** button.

Using the Security System

7. In the next text entry field, enter a descriptive name for this PPTP connection.

Then click on the **Next** button.

8. In the **Start/Settings/Network and Dialup Connections**, a right-click on the new icon will allow you to open the **Properties** window and configure further options:

General: This allows you to change the hostname or destination address of the connection. In the **Connect First** window, select any network connections that need to be established before setting up the PPTP session.

Options: The dial and redial options can be defined here.

Security: Choose the **Advanced (Custom Settings)** option. Next click the **Settings** button. Leave these settings as they are.

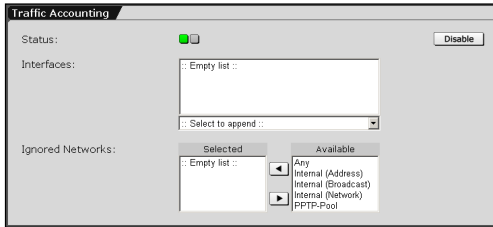
Network: In the **Type of VPN Server I am calling** menu, select the **Point-to-Point-Tunneling Protocol (PPTP)** option.

Sharing: This menu allows you to share the PPTP connection with other computers on the local network.

To start the PPTP connection, simply click the new icon in the **Start/Settings/Network and Dialup Connections** menu.

Further information is usually available from the network administrator.

5.3.7. Accounting



When the **Accounting** function is enabled, the security system will track all transmitted data and compile statistics about it. The accounting menu allows you to select which network

cards should be monitored. You can download the data from the **Log Files/Accounting** menu, or view daily reports in the **Reporting/Accounting** menu.

Important Note:

In the normal case, you should only enable **Accounting** on one network card, because, if more than one card is monitored, data forwarded from one monitored interface to another monitored one will be counted twice.

If you use **Masquerading**, you should probably use **Accounting** on the internal interface. Otherwise, data packets dropped by the security system filters will be included, and will appear to come from the wrong interface.

It is also possible to exclude certain **Hosts** or **Networks** from the **accounting** records. After installation, all networks are included in accounting records.

It may be useful to block certain hosts or networks from **accounting** data, for instance when a **DMZ** host only communicates with internal systems, but you are only interested in collecting **accounting** data for outbound traffic. Since it might only be used for internal means, it might not be useful to consider its traffic data.

In the **Reporting/Accounting** menu, you can monitor the collected **accounting** data and edit accounting rules.

Using the Security System

Important Note:

Do not use **accounting** on network interfaces. Doing so may overload the system.

Configuring Traffic Accounting:

1. In the **Network** tab, open the **Accounting** menu.
2. Enable the function by clicking the **Enable** button.
The status light will show green and another entry window will open.
3. In the **Interfaces** selection field, choose the network cards.
Please see chapter 4.3.2 on page 36 for a description of how to use **selection fields**.
4. Use the **Ignored Networks** selection menu to choose which networks to ignore.

The settings in the **Traffic Accounting** menu will immediately be enabled.

5.3.8. Ping Check



Ping allows you to test the connection with a remote host on the IP level. Please note that these tools require

that the **ICMP on firewall** option under the **Packet Filter/ICMP** menu be enabled. **Ping** sends an **ICMP Echo Packet** to the remote machine. When this packet is received by the remote machine, its TCP/IP stack will generate an **ICMP Reply Packet** and send it back. This allows you to test that IP-level connectivity with the remote machine.

Ping Check also allows you to check the connection with a host by entering the DNS hostname. In order to do that, **DNS Proxy** must be enabled in the **Proxies/ DNS** menu.

Note:

- **Ping** will not work unless **ICMP on firewall** (in the **Packet Filter/ICMP** menu) is activated.
 - **Name Resolution** will not work unless **DNS Proxy** (in the **Proxies/DNS** menu) is activated.
-

Using the Security System

Using Ping:

1. Under the **Network** tab, open the **Ping Check** menu.
2. Use the **Ping Host** drop-down menu to select a network card.
If this is an interface with a host, configured in one of the menus **Interfaces** or **Networks**, you can select it directly from the drop-down menu.
(Example: **Internal (Address)** for the internal network card on the security system).
For another host in the network, select the setting **Custom Hostname/IP Address** from the drop-down menu.
3. In the **Hostname /IP Address** entry field, enter the IP address or hostname.
4. Click **Start** to begin the test connection.

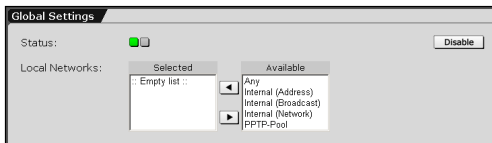
5.4. Intrusion Protection

The **Intrusion Protection System (IPS)** recognizes attacks with the help of a signature-based Intrusion Detection set of rules. The system analyzes the complete traffic and automatically blocks attacks before they can reach the network.

The existing set of rules and/or IPS attack signatures are updated through the **Pattern Up2Date** function. New IPS attack signatures will automatically be imported as IPS rule to the IPS set of rules.

5.4.1. Settings

Global Settings

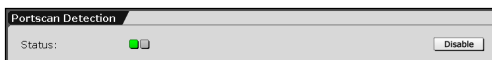


In the window, configure the basic settings for the **Intrusion Protection System (IPS)** option.

Status: Clicking on the **Enable** button enables the option.

Local Networks: From the selection field select those networks that should be monitored by the Intrusion Protection System (IPS). If no specific network is selected, the complete data traffic will be monitored.

Portscan Detection



The **Portscan Detection (PSD)** feature allows you to

detect possible attacks from unauthorized users. Portscans are used by hackers to probe secured systems for available services: In order to intrude into a system, or to start a **Denial-of-Service (DoS)** attack, attackers need information on network services. If this

Using the Security System

information is available, attackers might make use of the security deficiencies of these services. Network services using the TCP and UDP Internet protocols, can be accessed via special ports and this port assignment is generally known, for example the SMTP service is generally assigned to the TCP Port 25. The ports, used by the services are referred to as open, since it is possible, to establish a connection to them. Whereas unused ports are referred to as closed, every attempt to connect with them fails. The attacker tries to find the open ports with the help of a particular software tool, i.e. the Port Scanner. This program tries to connect with several ports on the destination computer. If it is successful, the tool displays the relevant ports as open and the attacker has the necessary information, showing him which network services are available on the destination computer.

The following is an example of the information returned by a port scanner:

Interesting ports on (10.250.0.114):

(The 1538 ports scanned but not shown below are
in state: closed)

Port	State	Service
25/tcp	open	smtp
135/tcp	open	loc-serve
139/tcp	filtered	netbios-ssn
445/tcp	open	Microsoft-ds
1032/tcp	open	iad3

Since 65535 ports are available for the TCP and UDP Internet protocols, the ports are scanned at very short intervals. When the firewall detects an unusually large number of attempts to connect to services, especially when these attempts come from the same source address, this is almost certainly due to a portscan.

PSD watches for such scans and immediately informs the administrator via e-mail when one is detected. The administrator can also decide what further measures should be taken in response to the

scan. The e-mail address of the administrator can be configured in the **System/Settings** menu.

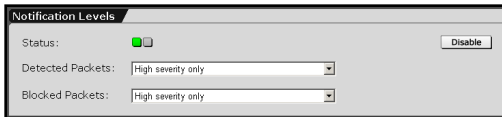


Security Note:

The administrator should take special care that all systems have the most recent security patches installed.

The Up2Date service, which updates the security system itself, is detailed in chapter 5.1.3 on page 54.

Notification Levels



If the **Intrusion Protection System (IPS)** detects IPS attack signatures or prevents an intrusion, the

system will send a message to the administrator. The e-mail address of the administrator can be configured in the **System/Settings** menu.

Detected Packets: Use this drop-down menu to select the severity level from which on a warning should be sent (Intrusion Detection).

- **All levels:** For each level of risk.
- **High and medium severity:** for high and medium levels of risk.
- **High severity only:** only for high risk levels.
- **None:** No warning will be sent.

Blocked Packets: Use this drop-down menu to select the level of risk, from which on a warning should be sent (Intrusion Prevention).

- **All levels:** For each level of risk.
- **High and medium severity:** for high and medium levels of risk.
- **High severity only:** only for high risk levels.
- **None:** No warning will be sent.

Using the Security System

5.4.2. Rules

The **Rules** menu contains the **Intrusion Protection System** set of rules (**IPS**). The already existing base set of rules with the IPS attack signatures can be updated through the **Pattern Up2Date** function, if desired. New IPS attack signatures will automatically be imported as IPS rule to the IPS rules table.

The **Pattern Up2Date** function is described in further detail in chapter 5.1.3 on page 54.

IPS Rules Overview

The overview contains all IPS sets of rules.

Intrusion Protection Rules			Total 2012 entries, 1968 filtered	▽ New Rule ... ▽	▽ Filters ▽
		▽ Group	Hits	Info	
		attack-responses	0	Recognition of successful attacks	
		backdoor	0	Rules for backdoor software	
		bad-traffic	0	Recognizes traffic that should never occur	
		chat	0	Recognition of messaging and chat traffic	
		ddos	0	Rules for Distributed Denial of Service	
		dns	0	Rules for DNS protocol	
		dos	0	Denial of Service attacks	
		exploit	0	Well-known exploits of specific software	
		finger	0	Rules for finger protocol	
		ftp	0	Rules for FTP protocol	
		icmp	0	Rules for ICMP protocol	
		icmp-info	0	Recognition of assumingly harmless ICMP traffic	

The functions in the overview from the left to the right:

: Clicking on the status light enables the IPS set of rules.

: The IPS rule can be configured as alarm rule (Intrusion Detection) or as blocking rule (Intrusion Prevention). Clicking on the icon switches the application of the IPS rules in this group.

: Clicking on the folder icon opens the sub-tab with all protocols of this group.

By clicking again on the icon, you will get back to the overview. The

additional functions in the sub-tab are described in the „IPS Rules Sub-tab“ section.

Group: The name of the IPS group of rules is displayed in this column. The groups are put in alphabetical order according to this name. Clicking in the header automatically displays the groups in descending or increasing alphabetical order.

Hits: This column displays, how often a rule from the group became active.

Info: This column provides short information on this IPS rule group.

The IPS Rule Sub-tab

All IPS rules of a group are listed in this sub-tab. The sub-group can be opened in the overview by clicking on the folder icon (📁).

			ddos	0	Rules for Distributed Denial of Service
			dns	0	Rules for DNS protocol
			dos	0	Denial of Service attacks
			exploit	0	Well-known exploits of specific software

Intrusion Protection Rules			Total 2012 entries, 1992 filtered		▽ New Rule ... ▽	▽ Filters ▽
		▽ Group	Hits	Info		
			dns	0	Rules for DNS protocol	
			dns	0		DNS EXPLOIT named overflow (ADMROCKS) - ID 260
			dns	0		DNS EXPLOIT x86 Linux overflow attempt - ID 262
			dns	0		DNS zone transfer TCP - ID 255
			dns	0		DNS EXPLOIT x86 Linux overflow attempt - ID 264
			dns	0		DNS EXPLOIT named tsig overflow attempt - ID 303
			dns	0		DNS named version attempt - ID 257
			dns	0		DNS EXPLOIT named overflow (ADM) - ID 259
			dns	0		DNS SPOOF query response with TTL of 1 min. and no authority - ID 254
			dns	0		DNS EXPLOIT x86 Linux overflow attempt (ADMv2) - ID 265

The functions in the sub-tab from the left to the right:

/ : Clicking on the status light enables the IPS rule.

/ : The IPS rule can be configured as alarm rule (Intrusion Detection) or as blocking rule (Intrusion Prevention). Clicking on the icon switches the application of the IPS rule in this group.

Using the Security System



: Return to the overview by clicking on the folder icon.

Group: The name of the IPS group of rules is displayed in this column.

Hits: This column displays, how often a rule from the group became active.

Info: The first line provides short information on this IPS rule group. You can obtain detailed information on the IPS rules by clicking on the correspondent icon with the mouse.



: This window presents the parameters of this as Low Layer Information.



: Clicking on the icon connects you to the correspondent link in the Internet. The Website contains further information on the IPS rule. This information is compiled in projects such as Common Vulnerabilities and Exposures (CVE) and published in the Internet.

Setting an IPS rule:

You can add your own IPS rules to the set of rules. The rules are based on the syntax of the Snort Open Source ID System. Manually configured IPS rules are always **locally** imported to an IPS set of rules. For more information please see the following Internet address: <http://www.snort.org>.

1. Under the **Intrusion Protection** tab, open the **Rules** menu.
2. Click on the button.

The entry window will open.

3. Make the following settings:

Intrusion Protection Rules
Total 2012 entries, 1968 filtered
△ New Rule ... △
▽ Filters ▾

Description:

Selector:

Filter:

Hint: Local rules will be added to the **local** group.

☐
☐
☐
☒

▽ Group

Hits

Info

☒
☐
☐
☐

attack-responses

0

Recognition of successful attacks

Description: Enter a description of the rule in the entry field.

Example: Large ICMP packet

Selector: Enter the selection parameters for the IPS rule in the Snort syntax in the entry field.

Example: icmp \$EXTERNAL_NET any -> \$HOME_NET any

Filter: Enter the real identification parameter for the IPS rule in Snort syntax in the entry field. Please make sure that the entry ends with a ;-sign.

Example: dsize: >800;

4. Save your configuration by clicking **Add local Rule**.

The new **IPS rule** is always **locally** imported to an IPS set of rules. The rule is immediately enabled (status light shows green).

<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	info	0	Informational messages
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	local	0	Locally generated rules
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	misc	0	Miscellaneous rules
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	multimedia	0	Recognition of multimedia streaming software

			▽ Group	Hits	Info
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	local	0	Locally generated rules
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	local	0	example - ID 10000

Using the Security System

5.4.3. Advanced

The screenshot shows a configuration window with two tabs: "Policy and Exclusions" and "Performance Tuning".

Policy and Exclusions Tab:

- Policy:** A drop-down menu currently set to "Drop silently".
- IPS Network Exclusions:** A section showing "Total 0 entries" and a "New Exclusion ..." button.

Performance Tuning Tab:

- HTTP Service:** A drop-down menu with the text "Please select".
- HTTP Servers:** A list management interface with "Selected" and "Available" columns. The "Selected" column is empty. The "Available" column lists: "Any", "Internal (Address)", "Internal (Broadcast)", "Internal (Network)", and "PPTP.Pool".
- DNS Servers:** A list management interface with "Selected" and "Available" columns. The "Selected" column is empty. The "Available" column lists: "Any", "Internal (Address)", "Internal (Broadcast)", "Internal (Network)", and "PPTP.Pool".
- SMTP Servers:** A list management interface with "Selected" and "Available" columns. The "Selected" column is empty. The "Available" column lists: "Any", "Internal (Address)", "Internal (Broadcast)", "Internal (Network)", and "PPTP.Pool".


This menu allows you, to configure additional settings for the **Intrusion Protection System (IPS)**. This should, however, only be done by experienced users.

Policy and Exclusions

Policy: From this drop-down menu select the security policy that the Intrusion Protection System should use, if a blocking rule detects an IPS attack signature.

- **Drop silently:** The data packet will only be blocked.
- **Terminate connection:** A TCP Reset and/or ICMP Unreachable (for UDP) packet will be sent to both communication partners and the connection will be terminated.

IPS Network Exclusions: Specific connections between the networks of the Intrusion Protection System (IPS) can be excluded in this selection menu.

The connections will be listed in a table below the selection menu. Clicking the trash can icon () deletes the defined connection from the table.

Performance Tuning

The performance of the *Intrusion Prevention System (IPS)* can be enhanced through the settings in this window, in which the servers and ports are defined. The correspondent IPS rules will only be used for the configured servers and ports.

The server must first be added as host in the **Definitions/Networks** menu. For more information on adding hosts, please refer to chapter 5.2.1 on page 103.

Note:

If you don't configure a server in this window, the **Intrusion Protection System (IPS)** will monitor the complete data traffic according to the settings in the **Global Settings** window.

HTTP Service: In this drop-down menu select the target port for the HTTP data traffic, by selecting a *Service*. In the **Definitions/Services** menu, you can change or add a *Service*, if necessary. The added service will only use the target port number. In the case of a port range, only the first and last port will be used.

Example: In a port range 80:8080 the HTTP rule will be used for the target port 80 and 8080.

HTTP Servers: Select the HTTP servers in this selection field.

DNS Servers: Select the DNS servers in this selection field.

SMTP Servers: Select the SMTP servers in this selection field.

SQL Servers: Select the SQL servers in this selection field.

Telnet Servers: Select the Telnet servers in this selection field.

Using the Security System

5.5. Packet Filter

The **Packet Filter** is the central part of the firewall. In the **Rules** menu you define the allowed data traffic between the networks and hosts in the form of **Packet filter rules**. You can also define specific packets, which will never be allowed to pass through the firewall. The packet filter management is done in the **Rules table**.

The tools in the **ICMP** menu allow you to check the network connections and functions of the security system. The additional and reporting functions are available in the **Advanced** menu.

5.5.1. Rules

	Group	Source	Service	Action	Destination	Comment
1	[none]	Marketing	HTTP	allow	Any	Example rule

The **Rules** menu allows you to define packet filter sets of rules. These rules are defined with the help of the **network** and **service** definitions.

In general, there are two basic kinds of packet filtering policy:

- Default allow – the rules explicitly define which packets are blocked; all others are allowed.
- Default deny– the rules explicitly define which packets are allowed; all others are dropped.

This security system uses a **Block all packets** policy, as this policy is inherently much more secure. This policy requires you to define explicitly, which IP packets will be allowed to pass the filter. All other packets will be blocked and – depending on the action chosen – displayed in the **Packet Filter Live Log**. The **Packet Filter Live Log** is contained in the menu **Packet Filter/Advanced**.

Example:

Network A is a subset of network B. Rule 1 allows SMTP traffic destined for Network A. Rule 2 blocks SMTP for network B. Result: Only SMTP traffic for network A will be allowed. SMTP packets from the rest of network B IP addresses will be blocked.

A packet filter rule is defined by the **source address (Source)**, a **service (Service)**, the **destination address (Destination)** and a **Response (Action)**.

The following values can be chosen as source and target addresses. Please see the corresponding chapters of this for a more detailed explanation of how to configure and manage these targets.

- A **Network** – networks are defined in the **Definitions/Networks** menu.
- A **Network Group** – network groups are defined in the **Definitions/Network** menu.
- An **Interface** network – logical networks are defined automatically by the system when configuring a new network card or interface. Interfaces can be configured in the **Network/Interfaces** menu.
- An **IPSec Remote Key Object (IPSec User Group)** – the IPSec User groups are defined in the **Definitions/Networks** menu. This address or port range is required when configuring packet filter rules for IPSec Road Warrior Endpoints.

A new defined packet filter rule is initially disabled, when it is added to the table. Active rules are applied in the given order, ending with the first matching rule. The order of this process will be displayed in the table through the **Position number** (second column from the left). If you re-sort the rules table later, for example according to the *source address* please, note that the rules won't be displayed in the order in which the system processes the rules. If, however, you change the numerical rule order via the **Position number**, the processing order will change correspondingly. In our example, if rule

Using the Security System

2 were moved to be before rule 1, all SMTP traffic for both networks would be blocked. Be very careful when defining rules and their order, as this will determine the security of your firewall.

Important Note:

When one filter rule applies, all other rules will be ignored! The sequence of rules is thus very important. Never place a rule like **Any** (Source) – **Any** (Service) – **Any** (Destination) – **Allow** (Action) at the top of the rule set.

Setting Packet Filter Rules:

1. Under the **Packet Filter** tab, open the **Rules** menu.
2. Click on the **New** button.

The entry window will open.

ID	Group	Source	Service	Action	Destination	Comment
1	[none]	Marketing	HTTP	Allow	Any	Example rule

3. Make the following settings:

Position: Define the line of the table, in which the packet filter rule will be entered. It is possible, to change the sequence of the packet filter rules later. By default, the rule is placed at the end (**To Bottom**) of the rules table.

Group: For a smooth management of the set of rules, the packet filter rules can be grouped together in one group. This does not influence the way, in which a rule will be processed within the set of rules.

For the first rule, no group can be selected from the drop-down menu yet. New groups are defined in the set of rules table.

Source: In the drop-down menu, select the source address of the data packets. The **Any** setting applies to all IP-addresses, regardless of whether these are publicly assigned IP-addresses or private IP-addresses according to RFC1918.

Service: Use the drop-down menu to select a service.

This list includes all the pre-defined services included in the Security system, as well as the ones that you defined yourself. This allows you to define precisely which traffic should be allowed. The **Any** setting represents here all combinations of protocols and source and/or destination ports.

Destination: In the drop-down menu, select the source address of the data packets.

The **Any** setting applies to all IP-addresses, regardless of whether these are publicly assigned IP-addresses or private IP-addresses according to RFC1918.

In the **Action** drop-down menu, select the action to execute if a data packet complies with the settings for **Source**, **Service** und **Destination**: In connection with this action, the priority for the **Quality of Service (Qos)** function is also configured here.

Important Note:

In order to enable the priorities **high priority** and **low priority**, you must select the respective interface for the **QoS** function in the **Network/Interfaces** menu and also define the values **Up-link Bandwidth (kbits)** and **Downlink Bandwidth (kbits)**.

Allow: All packets, complying with this rule are allowed to pass.

Using the Security System

Allow (high priority): All packets, complying with this rule are allowed to pass. In addition, this data traffic gets a higher priority if the Uplink is overloaded.

Allow (low priority): All packets, complying with this rule are allowed to pass through. In addition, this data traffic gets a lower priority if the Uplink is overloaded.

Drop: All packets matching this rule are blocked.

Reject: All packets, complying with this rule are denied. In addition, the firewall will send an ICMP error to the sending computer.





Log: Any violation of the rule will be reported in the **Packet Filter Live Log**. This action is enabled by clicking on the check box.

For such filter violations, which take place very often, and which are not particularly security-relevant and only reduce the readability of the **Packet Filter Live Log** (e.g. Windows NetBIOS broadcasts), we recommend not to enable the **Log** function.

Comment: In this entry field you can optionally enter a comment on a rule.

4. Save your configuration by clicking **Add Definition**.

If the definition was successful, the new **Packet filter rule** will be added to the rule table in a deactivated state, marked by the red status light.

	△	Group		Source	Service	Action	Destination	Comment
	1	[none]		Marketing	 HTTP		 Any	 Example rule

5. Activate the Packet filter rule by clicking the status light.

After the rule is added to the table, further options are available for managing and editing rules in the rules table.

Note:

By default, new rules are added in an **inactive** state in the table. The rule will only become effective when it is set to be **active**. See **Activating/deactivating rules**.

The Rules Table

Each packet filter rule will be displayed in the table through a separate line: The different settings will either be displayed as alphanumeric signs or as symbols. While all settings with alphanumeric signs can be edited by clicking on the correspondent field, this is not possible with all symbol displays.






		Group		Source		Service		Destination		Comment
	1	[none]		Marketing		HTTP				Example rule

The following table explains all symbols from the rules table:

The Symbols

Icon	Spalte	Anzeige/Einstellung
		Trash can
	Status light	Packet filter rule is disabled
	Status light	Packet filter rule is enabled
	Source/Destination	Host
	Source/Destination	Network
	Source/Destination	Network group
	Source/Destination	DNS Hostname
	Source/Destination	IPSec User Group
	Action	Allow
	Action	Allow (high priority)

Using the Security System

Icon	Spalte	Anzeige/Einstellung
	Action	Allow (low priority)
	Action	Drop
	Action	Reject
	Log	Log disabled
	Log	Log enabled

Adding/editing groups: Clicking in the field in the **Group** column opens an entry window. Clicking on the **Save** button saves your changes.

To cancel this service click on the **Cancel** button.

Enabling/Disabling Packet filter rules: The status light in the fourth column shows the rule status. Clicking the status light toggles the state between **active** (green light) and **inactive** (red light). Deactivated rules remain in the database, but have no effect on firewall behavior.

Edit rules: Clicking on the correspondent setting will open an entry window. The rule can then be modified. Click **Save** to save your changes.

In order to interrupt this process, click on the **Cancel** button.

Re-order rules: The order of the rules in the table determines the behavior of the firewall; having the correct order is essential for secure operation. By clicking the position number, you can adjust the order to suit your needs. In the drop-down menu select the Position, to which you wish to place the packet filter rule and confirm your settings by clicking on the **Save** button.

Delete rules: Click the trash can icon to delete a rule from the table.

Sorting the rules table: By clicking on the column headers, you can sort the table: for instance, to sort the rules by sender address, click

Source. To return to the precedence-based sorting **Matching**, click the column with the position numbers.

Filters

The **Filters** function allows you to filter *Packet Filter Rules* by specific attributes. This function enhances the management of huge networks with extensive sets of rules, since rules of a specific type can be presented in a concise way.

Filtering rules:

1. Click on the **Filters** button.
2. The entry window will open.
3. Enter the filter attributes in the fields. Not all attributes must be defined.

Group: If you want to filter the rules of a specific group, select them from the drop-down menu.

State: This drop-down menu allows you to filter rules by a specific status.

Source: This drop-down menu allows you to filter rules by a specific source address.

Service: If you want to filter rules by a specific service, select it from the drop-down menu.

Action: This drop-down menu allows you to filter rules by a specific action.

Destination Port: This drop-down menu allows you to filter rules by a specific destination address.

Log: This drop-down menu allows you to filter logged rules.

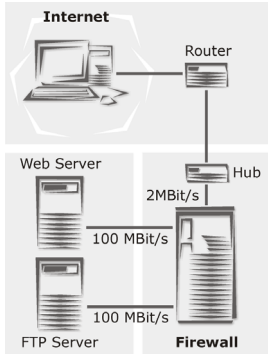
Comment: If you want to filter services by specific comments, enter the expressions in the entry menu.

4. To start the filter click on the **Apply Filters** button.

Using the Security System

Only the filtered packet filter rules will be displayed then. When the menu is closed, the complete set of rules will be displayed again.

Quality of Service (QoS)



Internet Service Providers usually measure the service they provide in terms of bandwidth, measured in kBit/s. If a server tries to cross the saturation boundary – if it tries to send more information than the link can carry – the communication can either slow to a crawl or be dropped altogether.

The graphic at left, for example, shows a network with a web server and an FTP server. Both servers share a 2Mbit uplink to the Internet. Due to the protocols, TCP based applications (e.g. FTP) always use the full bandwidth. It might thus happen that not enough bandwidth is available for the Web Server.

The **Quality-of-Service-(QoS)** function allows you to assign different priorities to the connections, if the Uplink is overloaded. These priorities are defined in the packet filter rules through the **Allow, Allow (high priority)** and **Allow (low priority)** actions.

Important Note:

In order to enable the priorities **high priority** and **low priority**, you must select the respective interface for the **QoS** function in the **Network/Interfaces** menu and also define the values **Uplink Bandwidth (kbits)** and **Downlink Bandwidth (kbits)**.

Using the Security System

In order to assign the same bandwidth to the connection with the web server, as shown in the example, as the one for the connection with the FTP server, both packet filter rules must be set to the same

Action:

1. Rule for data packets from the web server:

Source: web server

Service: HTTP

To (Server): Internet

Weight: Allow (high priority)

2. Rule for data packets from the FTP server:

Source: FTP server

Service: FTP

Destination: Internet

Action: Allow (high priority)

	△	Group		Source		Service	Action		Destination		Comment
	1	[none]		Marketing		HTTP			Any		Example rule
	2	[none]		Web Server		HTTP			Any		QoS Example rule
	3	[none]		FTP Server		FTP			Any		QoS Example rule

If the Uplink is only used by the data packets of these two servers, each connection receives one half of the bandwidth (1MBit/s) in the **Worst Case**. The **High Priority** setting becomes only relevant, if a third data connection is established. All connections with a lower priority, **Allow** or **Allow (low priority)**, will be treated with a lower ranking.

Using the Security System

Additional Functions and Settings

Internet-wide Broadcast:

In order to **drop IP broadcast** packets, first define the broadcast address in the **Definitions/Networks** menu in the form of a new network. Next, install the appropriate packet filter rule and activate it.

1. Under **Definitions**, open the **Networks** menu and define the following network:

Name: Broadcast32

Type: Host

IP Address: 255.255.255.255

Comment (optional): Enter a comment.

2. Confirm the entries by clicking **Add Definition**.
3. Under **Packet Filter**, open the **Rules** menu and enter the following rule:

Source: Any

Service: Any

Destination: Broadcast32

Action: Drop

Comment (optional): Enter a comment.

4. Confirm the entries by clicking **Add Definition**.

Segment-wide Broadcast:

For each network card configured in the Interfaces menu, the system automatically defines a network named **NAME (Broadcast)**.

For more information, please see the **Current Interface Status** section of chapter 5.3.2 on page 119.

1. Under **Packet Filter**, open the **Rules** menu and enter the following rule:

Source: Any

Service: Any

Destination: Select the broadcast network for the relevant interface here.

Example: NAME (Broadcast)

Action: Drop

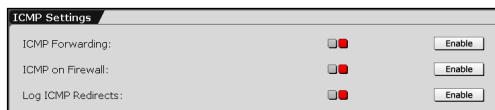
Comment (optional): Enter a comment.

2. Confirm the entries by clicking **Add Definition**.

Using the Security System

5.5.2. ICMP

ICMP Settings



This menu is used to configure the settings for **Internet Control Message Protocol (ICMP)** packets:

ICMP is used for testing network connectivity and troubleshooting network problems.

Note:

More information on **ICMP** can also be found in the **Ping** and **Traceroute** sections.

ICMP on firewall and **ICMP forwarding** apply to all IP addresses (**Any**). When **ICMP on firewall** is activated (green status light), all IP addresses can ping the firewall; when **ICMP forwarding** is enabled, computers on the external network can ping hosts behind the firewall. Pings to single IP addresses cannot then be blocked with packet filter rules.

Important Note:

Settings configured here take precedence over rules configured in the packet filter rules table.

When the **ICMP** settings are disabled, packet filter rules can be used to allow specific IP addresses or networks to ping the firewall or internal network.

ICMP Forwarding: This allows you to forward all ICMP packets behind the firewall. This means, that all IPs in the local network and in all connected DMZs can be pinged.

Click the **Enable** button to enable the function (status light shows green).

Important Note:

If you wish to disable **ICMP forwarding**, you must ensure that the **Packet Filter/Rules** menu does not contain a rule of the form **Any** (*Source*) – **Any** (*Service*) – **Any** (*Destination*) – **Allow** (*Action*). Otherwise **ICMP forwarding** will remain active irrespective of the setting here.

ICMP on Firewall: The firewall directly receives and forwards all ICMP packets. This is enabled by default (status light shows green). Click the **Disable** button to change disable the function (status light shows red).

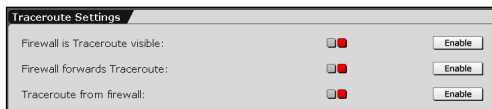
Note:

ICMP on firewall must be activated to use the **Ping** action. The action is described in more detail in the **Network/Ping Check** menu and is described in chapter 5.3.8 on page 177.

Log ICMP Redirects: **ICMP Redirects** are sent from one router to the other, in order to find a better route for a destination. Router then change their routing tables and forward the following packets to the same destination on the supposed better route.

This function logs the *ICMP Redirects*. Clicking on the **Enable** button enables the function (status light is green).

Traceroute Settings



Traceroute is a tool used to check and troubleshoot network routing. This tool can resolve the path to an IP

address. Traceroute lists the IP addresses of the routers that had been used to transport the sent packet. Should the packet path not be reported within a certain time interval, traceroute will report a star (*) instead of the IP address. After a certain number of failures, the

Using the Security System

test will end.

An interruption of the test can have any number of causes, notably a packet filter along the network path that blocks traceroute packets.

This window shows advanced options related to **ICMP Traceroute**. The settings here can also open the UDP ports **UNIX Traceroute** uses.

Firewall is Traceroute visible: When this function is enabled, the firewall will respond to **Traceroute** packets.

Click the **Enable** button to enable the function (status light shows green).

Firewall forwards Traceroute: When this function is enabled, the firewall will forward **Traceroute** packets.

Click the **Enable** button to enable the function (status light shows green).

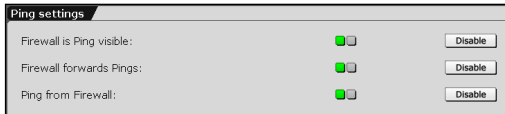
Note:

These two functions, **Firewall is Traceroute visible** and **Firewall forwards Trace route**, are probably only useful when both are enabled.

Traceroute from Firewall: The Traceroute command can be used on the firewall.

Click the **Enable** button to enable the function (status light shows green).

Ping Settings



This window contains configuration options specific to **ICMP Ping**.

Further information about **Ping** can be found in chapter 5.3.8 on page 177.

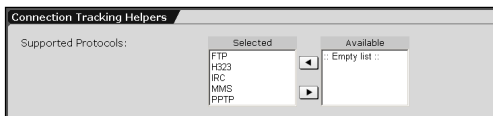
Firewall is ping visible: When this function is enabled, the firewall will respond to **Ping** packets. Click the **Enable** button to enable the function (status light shows green).

Firewall forwards Ping: When this function is enabled, the firewall will forward **Ping** packets. Click the **Enable** button to enable the function (status light shows green).

Ping from Firewall: The **Ping** command can be used on the firewall. Click the **Enable** button to enable the function (status light shows green).

5.5.3. Advanced

Connection Tracking Helpers



The **Stateful Inspection Packet Filter** and the **NAT** function are provided by the *iptables* module in the *Net-*

filter sub-system. All connections, operated with the packet filter, will be tracked by the *Conntrack* module: this is referred to as **Connection Tracking**.

Some protocols, such as FTP or IRC require several communication channels, which cannot be connected through port numbers. In order to use these protocols with the *Packet filter*, or to replace an address through *NAT*, the **Connection Tracking Helpers** are required.

Using the Security System

Helpers are structures, referring to so-called Conntrack Helpers. Generally speaking these are additional Kernel modules that help the Conntrack module to recognize existing connections.

For FTP data connections, a FTP Conntrack helper, for example, is necessary. It recognizes the data connections, belonging to the control connection (normally TCP Port 21), which can have any destination port and adds the respective expect structures to the expect list.

The following protocols are supported. By default, all Helper modules are loaded:

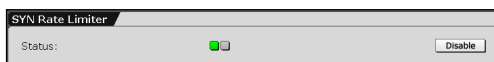
- FTP
- H323
- IRC (for DCC)
- MMS (Microsoft Media Streaming)
- PPTP

Loading Helper Modules: By default, all Helper modules are loaded.

The helper modules are loaded and deleted in the selection field.

A description of how to use the **selection fields** can be found in chapter 4.3.2 on page 36.

SYN Rate Limiter



Denial-of-Service attacks (**DoS**) on servers, shall deny the service access to

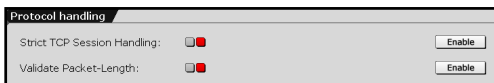
legitimate users. In the simplest case, the attacker overloads the server with useless packets, to overload its performance. Since a large bandwidth is required for such attacks, more and more

attackers start using so-called SYN-Flood attacks, which don't aim at overloading the bandwidth, but at blocking the system resources. For this purpose, they send so-called SYN packets to the TCP port of the service, i.e. in a web server to Port 80.

The **SYN Rate Limiter** function reduces the number of SYN packets, sent to the local network. This is disabled by default (status light shows red).

Click the **Enable** button to enable the function (status light shows green).

Protocol Handling



Strict TCP Session Handling: To secure a reliable data transport, the Trans-

mission Control Protocol (TCP) that is in the transport layer is used. TCP then creates computer to computer connections and continues to send data, until it receives an affirmative answer that the data have been transmitted. This type of connection is called **TCP Handshake** and is executed in three steps. Before a client is able to exchange data, with a server, for example, he sends a TCP packet, in the header of which there is also a so-called SYN-Bit (sequential number). This is an order to the server, to set up a connection. In addition, the client transmits the so-called window size. This value defines the maximum number of bytes for the usable data in the data package, so that they can be processed on the client. In the second step the server replies by setting an ACK-Bit (Acknowledge) to the header and also transmits the window size. In the last step, the client accepts this with the ACK-Bit and starts to send the data themselves.

The firewall accepts PSH packets without having received a **TCP Handshake**. This is necessary, if, for example after a **Restart** of the Internet security system or after a transfer of the second firewall system with a **High-Availability** system the existing connections shall be maintained.

Using the Security System

If the **Strict TCP Session Handling** function is enabled, the connection set-up is done by **TCP Handshake**.

Validate Packet-Length: The Packet Filter checks the data packets for minimal length if the icmp, tcp or udp protocol is being used.

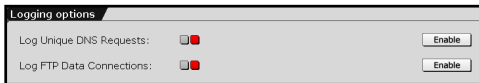
The minimal data lengths for the individual protocols are:

- icmp: 22 bytes
- tcp: 48 bytes
- udp: 28 bytes

If the data packets are shorter than the minimal values, they are blocked and recorded to the **Packet Filter** log file with the annotation **INVALID_PKT:**.

The log files are administered in the **Local Logs/Browse** menu.

Logging Options



Log Unique DNS Requests:

DNS packets, which are sent to or through the Firewall and

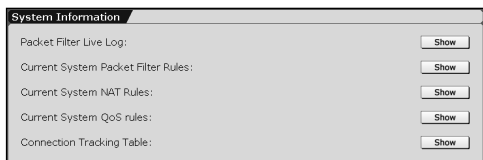
receive a DNS request are recorded to the **Packet Filter** log file with the annotation **DNS_REQUEST:**.

The log files are administered in the **Local Logs/Browse** menu.

Log FTP Data Connections: All FTP data connections – either in the Active or in the Passive mode – are recorded to the **Packet Filter** log file with the annotation **FTP_DATA:**.

The log files are administered in the **Local Logs/Browse** menu.

System Information



Packet Filter Live Log: The **Packet Filter Live Log** monitors the **packet filter** and **NAT** rules in place on the Security system. The window

provides a real-time display of packets intercepted by the packet filter. This is especially useful in troubleshooting and debugging packet filter rules. If, after the security system starts, a networked application, such as online banking, is not accessible, the Packet Filter Live Log can help you reconstruct which packets are being blocked by the packet filter.

Time	Action	Source IP-Address	Port	Destination IP-Address	Port	Protocol	TCP-Flags/ICMP-Type/HWADDRs
13:25:52	ACCEPT	10.113.113.5	1157	-> 192.168.5.217	443	TCP	SYN
13:25:53	ACCEPT	10.113.113.5	1158	-> 192.168.5.217	443	TCP	SYN
13:25:53	ACCEPT	10.113.113.5	1159	-> 192.168.5.217	443	TCP	SYN
13:25:53	ACCEPT	10.113.113.5	1160	-> 192.168.5.217	443	TCP	SYN
13:25:53	ACCEPT	10.113.113.5	1161	-> 192.168.5.217	443	TCP	SYN
13:25:53	ACCEPT	10.113.113.5	1162	-> 192.168.5.217	443	TCP	SYN
13:25:53	ACCEPT	10.113.113.5	1163	-> 192.168.5.217	443	TCP	SYN
13:25:54	ACCEPT	10.113.113.5	1164	-> 192.168.5.217	443	TCP	SYN
13:25:54	ACCEPT	10.113.113.5	1165	-> 192.168.5.217	443	TCP	SYN
13:25:54	ACCEPT	10.113.113.5	1166	-> 192.168.5.217	443	TCP	SYN
13:25:54	ACCEPT	10.113.113.5	1167	-> 192.168.5.217	443	TCP	SYN
13:25:54	ACCEPT	10.113.113.5	1168	-> 192.168.5.217	443	TCP	SYN
13:25:54	ACCEPT	10.113.113.5	1169	-> 192.168.5.217	443	TCP	SYN
13:25:55	ACCEPT	10.113.113.5	1170	-> 192.168.5.217	443	TCP	SYN
13:25:56	ACCEPT	10.113.113.5	1171	-> 192.168.5.217	443	TCP	SYN
13:25:56	ACCEPT	10.113.113.5	1172	-> 192.168.5.217	443	TCP	SYN
13:26:04	ACCEPT	10.113.113.5	1173	-> 192.168.5.217	443	TCP	SYN
13:26:07	ACCEPT	10.113.113.5	1174	-> 192.168.5.217	443	TCP	SYN
13:26:11	ACCEPT	10.113.113.5	1175	-> 192.168.5.217	443	TCP	SYN
13:26:13	ACCEPT	10.113.113.5	1176	-> 192.168.5.217	443	TCP	SYN

start LiveLog

The **Current Packet Filter rules** and **Current NAT rules** editing fields show all current rules in place in the firewall kernel.

By clicking **Show** button, a new window will appear. This window shows a real-time display of packets that have been dropped by the security system.

Click the **stop Live Log/start Live Log** button to pause or unpause the real-time display.

Note:

Please note that only those processed rules will be filed in a protocol, for which the **Log** function has been enabled under **Packet Filter/Rules!**

Using the Security System

Current System Packet Filter Rules: The **Current Packet Filter rules** window provides detailed information for expert administrators. The table shows all rules in real time, including system generated ones, and is taken directly from the operating system kernel.

Current System NAT Rules: As with the current filter rules, **Current NAT rules** displays all user- and system-defined NAT rules.

Connection Tracking Table: This menu shows a list of all current connections and the connection parameters.

5.6. Application Gateways (Proxies)

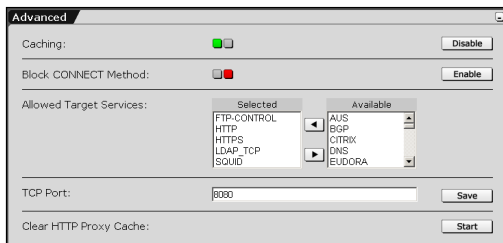
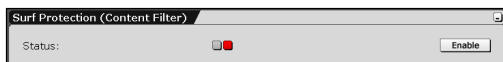
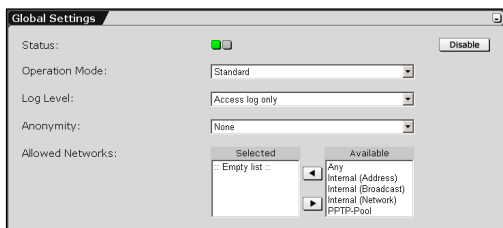
While a **Packet Filter** filters packets at the network level, **Proxies (also called Application Gateways)** offer control and security at the application level by preventing a direct connection between client and server.

Each **Proxy** can also provide further security services for its service. Since each proxy knows the context of its service, extensive security and protocol options are being offered. This intensive protocol analysis is made possible by well-defined and well-supported protocol standards. The proxies concentrate on the most essential information.

In the **Proxies** tab, select the **Proxies** with the same name and configure the settings. By default, all proxies are disabled. This security system contains proxies for **HTTP** (Web), **DNS** (Name server), **SOCKS** (point-to-point connections), **POP3**, **SMTP** (e-mail), and **Ident**.

Using the Security System

5.6.1. HTTP/Surf Protection



The **HTTP** menu allows you to configure the security system as a **HTTP Caching Proxy**. This proxy can provide caching services in addition to simple proxy ser-

vices, resulting in dramatic performance increases: because the system can store a copy of often-visited pages locally, these pages do not need to be loaded across the Internet.

Note:

WebAdmin should not be used through a proxy. Configure your browser so that connections to the security system's IP address do not use a proxy server.

Disabling Netscape Communicator, Proxy:

1. In Netscape, open the **Edit/Settings/Advanced/Proxies** menu.
2. Under **Manual Proxy Configuration** click **Show**.
3. In the **No Proxy for this address** field, enter the IP address of your security system.
4. Click **OK** to save your changes.

Disabling Proxy Use with Microsoft Explorer:

1. In Explorer, open the **Extras/Internet Options** menu.
2. Choose the **Connections** tab.
3. Open the **LAN Settings/Advanced** menu.
4. Under **Exceptions**, enter the IP Address of your security system.
5. Click **OK** to save your settings.

The **HTTP proxy** controls web transactions using the HTTP Protocol (usually TCP/IP Port 80). Please note that some web servers transmit some data, in particular streaming video and audio, over a port other than 80. These requests will not be noticed when the proxy is in **Transparent** mode: to support such requests, you must either use a different mode, or enter an explicit rule in the **Packet Filter/Rules** allowing them.

Example:

Source: a local network

Service: service with target address (the service must first be defined in the **Definitions/Services** menu)

Destination: IP address of the web server (or **Any**)

Action: Allow

HTTPS (TCP/IP Port 443) data is passed directly through the security system without processing.

Note:

In order to use the **Proxy** in **Standard** mode, the client **Browser** must be configured with the **TCP/IP Address** of the **security system** and the proxy **port** configured in the **Proxies/HTTP** menu. In addition, the HTTP proxy service requires a valid **Name server (DNS)**. Without configuring the client browser, the **Proxy** can only be used in **Transparent** mode.

Using the Security System

Global Settings

Operation Modes:

Standard: In this mode, you must select all networks which should be allowed to use the HTTP proxy service. If a browser on a non-configured network is configured to use the proxy, it will have no access to HTTP services.

If a browser on a non-proxied network is not configured to use the proxy, an appropriate packet filter rule can allow (un-proxied) access to HTTP services.

Example:

Source: IP address of a local client

Service: HTTP

Destination: IP address of the web server or **Any**

Action: Allow

To use the proxy, configure the client browser proxy settings to use the IP address of the security system and port 8080.

Transparent: In this mode, the system notices HTTP requests on the internal network, automatically processes them, and forwards them to the remote server. The client browser is entirely unaware of the proxy server. The advantage of this mode is that no additional administration or configuration is required on the client; the disadvantage is that only pure HTTP (port 80) requests can be forwarded.

All networks allowed to use the transparent proxy must be explicitly listed in the **Allowed Networks** menu. When **Transparent** mode is used, the client browser settings cannot be used to control proxy settings. Moreover, no data can be downloaded from a FTP server in this mode. HTTPS connections (SSL) must be executed via a Packet Filter.

User Authentication: This mode complies with the functions of the **Standard** mode. In addition, user access to the HTTP proxy is only authorized after previous **Authentication**.



Note:

Changes in **Proxies** become effective immediately, without further notice.

Enabling the HTTP Proxy:

1. In the **Proxies** tab, open the **HTTP** menu.
2. Enable the proxy by clicking the **Enable** button in the **Global Settings** window.

Another entry window will open.

3. In the **Operation mode** drop-down menu, select the mode to use.

Note again that some modes require client-side configuration. The modes are described in chapter "Operation Modes".

Having set the **Standard** or **Transparent** mode, continue with step 5.

4. If you have selected the **User Authentication** mode in the **Operation mode** drop-down menu, define the method of user authentication to use here.

Authentication Methods: Only those authentication methods that you have configured in the **Settings/User Authentication** menu are available here.

If you have configured the **Local Users** method, use the **Allowed users** selection menu to choose users allowed to use the proxy. **Local users** are defined in the **Definitions/ Users** menu.

5. In the **Log level** drop-down menu, choose the appropriate level of logging.

Full: All relevant information is recorded.

Using the Security System

Access Log only: The log only records access information, for example URL accessed and username/IP address of the client.

None: No information about the proxy use is recorded.

6. The **Anonymity** drop-down menu allows you to choose how much information about the client is passed on to the remote server in HTTP Request Headers.

Standard: The following headers are blocked: Accept-Encoding, From, Referrer, Server, WWW-Authenticate and Link.

None: Client headers are not changed at all.

Paranoid: All headers except those listed below are blocked. Additionally, the "User-Agent" field will be changed so that no information about the internal client is available.

Allow, Authorization, Cache-Control, Content-Encoding, Content-Length, Content-Type, Date, Expires, Host, If-Modified-Since, Last-Modified, Location, Pragma, Accept, Accept-Language, Content-Language, Mime-Version, Retry-After, Title, Connection, Proxy-Connection and User-Agent.

Note:

In **Standard** and **Paranoid** modes, the proxy blocks all cookies. If you wish to use cookies, you should use the **none** mode.

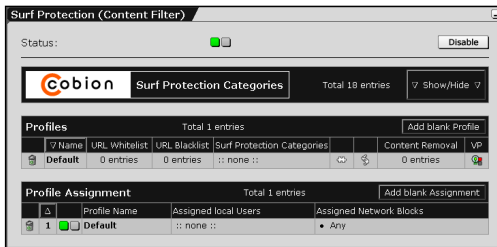
7. Use the **Allowed networks** selection menu to select which networks should be allowed to use the proxy.

A description of how to use the **selection field** tool can be found in chapter 4.3.2 on page 36.

All settings take effect immediately and will be saved if you leave this menu. Only the HTTP proxy can be accessed from the allowed networks.

See also the functions in the **Advanced** window.

Surf Protection (Content Filter)



The **Surf Protection Profiles** function allows you to produce profiles, which prevent access to certain web-sites. These profiles can then be associated with certain users or networks,

thus allowing control over which sites users may access. The categories are based on the **URL** data base from **Cobion Security Technologies** and can be edited in the **Surf Protection Categories** table.

Each *Surf Protection Profile* additionally contains a **Content Filter** with protection mechanisms.

Those protection mechanisms are:

- Virus Protection (VP)
- Embedded Object Filter
- Script Content Filter

This **Surf Protection** option can only be configured when the HTTP proxy is enabled.

Using the Security System

Surf Protection Categories

Cobion Surf Protection Categories		Total 18 entries	Δ Show/Hide Δ
7 Name	Subcategories		
Community_Education_Religion	<ul style="list-style-type: none">• Cities/Countries/Regions• Government Institutions• Non Government Organizations• Parties• Religion• Sects• Upbringing/Education/Reconnoitring		
Criminal_Activities	<ul style="list-style-type: none">• Computer Criminalism• Hate and Discrimination• Illegal Activities• Ware2 Sites		
Drugs	<ul style="list-style-type: none">• Alcohol• Illegal Drugs• Self Help/Addiction• Tobacco		
Entertainment_Culture	<ul style="list-style-type: none">• Art/Museums• Belletristics/Specialized Books• Cinema, TV• Humor• Music• Theme Parks		
Extremistic_Sites	<ul style="list-style-type: none">• Extrame		
Finance_Investing	<ul style="list-style-type: none">• Accumulation of capital/Investing• Banking/Homebanking• Brokerage/Stock Exchange		
Games_Gambles	<ul style="list-style-type: none">• Computer Games		

The **Surf Protection** option contains 17 defined **Surf Protection Categories**. The categories are based on the **URL** data base from **Cobion Security Technologies** and can be edited in this table.

Editing Surf Protection Categories:

1. Enable this option by clicking the **Enable** button in the **Surf Protection (Content Filter)** window.

The status light will show green and an advanced entry window will open.

2. Click the **Show/Hide** button to open the table with the categories.

The name of category is displayed in the **Name** field. This name will be selected later from the *Profiles Table*. The **Subcategories** field lists the subcategories.

3. Now click on the entry, you wish to edit.

Clicking on **Name** opens another entry window. If you click on the subcategories, another selection window will open. All available subcategories will be listed in this selection field.

▽ Name	Subcategories
<div>Community_Education_Religion</div> <div><div>Save</div><div>Cancel</div></div>	<ul style="list-style-type: none">• Cities/Countries/Regions• Government Institutions• Non Government Organizations• Partys• Religion• Sects• Upbringing/Education/Reconnoitring
Criminal_Activities	<ul style="list-style-type: none">• Computer Criminalism• Hate and Discrimination• Illegal Activities• Warez Sites

Save your changes by clicking on the **Save** button. To keep an entry, click **cancel**.

4. To close the table, click on the **Show/Hide** button.

The **Surf Protection Categories** window will close.

The Profiles Table

Each **Surf Protection Profile** will be displayed in the **Profiles** table through a separate line: The different settings will either be displayed as alphanumeric signs or as symbols. All settings can be edited by clicking on the correspondent field.

A **Surf Protection Profile** contains two function groups: The **Surf Protection Categories** with the additional functions *Blacklist*, *Whitelist* and *Content Removal*, and the **Content Filter**. The *Surf Protection Categories* prevent the access to Websites with a specific content. The *Content Filter* contains a *Virus Protection* function and filters Websites with specific technical components.


Using the Security System

The Functions

The following picture shows a **Surf Protection profile**:

Profiles		Total 1 entries			Add blank Profile	
	▽ Name	URL Whitelist	URL Blacklist	Surf Protection Categories		Content Removal VP
	Example	1 entries	0 entries	• Information_and_Communication  		0 entries 






The functions from the left to the right are:

Deleting Profiles (): Click on the trashcan icon to delete a profile from the table.

Name: This is the name of the Surf Protection Profile. This *Name* is necessary to assign this profile to a specific *Network* or *User*.

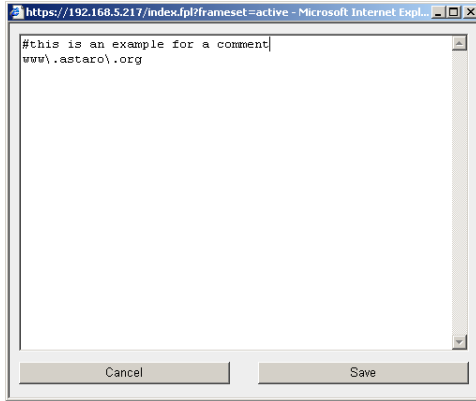
Open the editing window by clicking on the field with the entry (e.g. Default). Save your changes by clicking on the **Save** button. To keep an entry, click **cancel**.

URL Whitelist: This is an additional function from the **Surf Protection Categories**. With this access control list you can "allow" the access to specific Websites with a content that matches the subjects in the *Surf Protection Categories*.

Profiles		Total 1 entries			Add blank Profile	
	▽ Name	URL Whitelist	URL Blacklist	Surf Protection Categories		Content Removal VP
	Example	0 entries 	0 entries	• Information_and_Communication  		0 entries 

Example: If you have chosen the **Information and Communication** subject in the **Surf Protection Categories** menu, but wish to explicitly allow access to the **www.astaro.org** website, simply add this address to the **Whitelist**.

Using the Security System



Open the access control list by clicking on the field with the entry (e.g. 0 entries). Enter the Internet addresses one beneath the other into the entry field (e.g. www\astaro\org). Comments must be identified with a **#** sign at the beginning of each line. Save your changes by clicking on the **Save** button. To keep an entry, click **cancel**.

URL Blacklist: This is an additional function of the **Surf Protection Categories**. With this access control list you can "forbid" the access to specific Websites with a content that doesn't match the subjects in the *Surf Protection Categories*.

Open the access control list by clicking on the field with the entry (e.g. 0 entries). Enter the Internet addresses one beneath the other. Comments must be identified with a **#** sign at the beginning of each line.

Save your changes by clicking on the **Save** button. To keep an entry, click **cancel**.

Surf Protection Categories: In this field, choose the kinds of websites to which access should not be allowed.

Open the access control list by clicking on the field with the entry (e.g. 0 entries).

The **Surf Protection** option contains 17 defined **Surf Protection Categories**. Those 17 categories are administered and edited in the same table.

The administration of the **Surf Protection Categories** is described on page 216.

Using the Security System

Embedded Object Filter: This function deletes embedded objects such as ActiveX, Flash or Java from the incoming HTTP traffic.



Security Note:

Enable this function only, if high security demands apply to your network.



Clicking on the symbol enables () and disables () the **Embedded Object Filter**.

Script Content Filter: This function deletes script contents, such as Java and VBScript from incoming HTTP traffic.



Security Note:

Enable this function only, if high security demands apply to your network.



Clicking on the symbol enables () and disables () the **Script Content Filter**.

Content Removal: This is an additional function of the **Surf Protection Categories**. This access control list allows you to filter Web pages that contain specific expressions. Such texts, which contain an expression from the access control list, will be replaced by a HTML comment.

Open the access control list by clicking on the field with the entry (e.g. 0 entries). Enter the expressions one beneath the other. Comments must be identified with a **#** sign at the beginning of each line.

Save your changes by clicking on the **Save** button. To keep an entry, click **cancel**.

Virus Protection: This functions checks incoming traffic for dangerous content such as viruses.

Clicking on the symbol enables () and disables () the **Virus Protection**.

Enabling Surf Protection, adding Profiles:

1. Enable this option by clicking the **Enable** button in the **Surf Protection (Content Filter)** window.

The status light will show green and an advanced entry window will open.

By Default the **Profiles** table contains a **Blank Surf Protection Profile**.

2. To add a new **Blank Surf Protection Profile** to the table, click on the **Add blank Profile** button.

There you can edit the Surf Protection Profile.

Editing Surf Protection Profiles:

1. In the **Profiles** table go to the *Surf Protection Profile* that you wish to edit.
2. In the **Name** field enter a descriptive name for the *Surf Protection Profile*.
3. Now make the settings for the **Surf Protection Categories** functional group in the following order.

Surf Protection Categories: In this field, choose the websites topics to which access should be blocked from your network.

URL Whitelist: In the access control list enter those Internet addresses, for which you wish to "allow" access, even though their topic matches a topic in the **Surf Protection Categories** field.

URL Blacklist: In the access control list enter those Internet addresses, for which you wish to "forbid" access, even though their topic doesn't match a topic in the **Surf Protection Categories** field.

Using the Security System



Security Note:

In the HTTP protocol the header of the request will be filtered by the **HTTP Cache Proxy Squid**.

This is different in the **HTTPS** protocol - in this case, the squid does not read the header of the request, but performs a pass through. Therefore, the requested URL is unknown and cannot be filtered again. This means that the **Surf Protection** option cannot block **URLs** on the basis of **White-** or **Blacklists** for **HTTPS** connections.

Content Removal: In the access control list enter those expressions that should be deleted from the Web pages.

4. Make the settings for the **Content Filter** functional group.

Embedded Object Filter: Clicking on the symbol enables (🔒) and disables (🔓) the filter.



Security Note:

Enable the **Embedded Object Filter** function only, if high security demands apply to your network.

Script Content Filter: Clicking on the symbol enables (🔒) and disables (🔓) the function.



Security Note:

Enable the **Embedded Object Filter** function only, if high security demands apply to your network.

Virus Protection: Clicking on the symbol enables (🟢) and disables (🔴) the function.

The **Surf Protection Profile** is now edited. Now assign the profile in the **Profile Assignment** table to a *Network* or to a *Local User*.

The Profile Assignment Table

The **Surf Protection Profiles** from the **Profiles** table are assigned to Local Users or Networks in the **Profile Assignment** table.

To assign a *Surf Protection Profile* to a local user, the HTTP proxy must be used in the User Authentication Mode. The assignment of *Profiles* to a network is possible in every operation mode.

Important Note:

If you are simultaneously assigning a **Profile** to a **local user** and to a **network**, this *Profile* will only take effect, if the user accesses the HTTP proxy from the "configured" network! Only one **Surf Protection Profile** can be configured for each user or network.

If you have configured the **User Authentication** configuration mode in the **Global Settings** window, the **Profile Assignment via** drop-down menu will be displayed above the *Profile Assignment* table. By default this is set to **Local Users + Network blocks**.

If you have configured a radius or LDAP-Server in the **System/User Authentication** menu, they will be displayed in the drop-down menu. Once you have selected one of the servers, the **Profile Assignment** table will be masked.

Using the Security System

The Functions

The following picture shows a **Profile assignment**:

The screenshot shows a window titled "Profile Assignment" with a subtitle "Total 1 entries" and a button "Add blank Assignment". The window contains a table with the following columns: **Profile Name**, **Assigned local Users**, and **Assigned Network Blocks**. The first row has a trash icon, the number "1", a green status light, and the text "Example". The "Assigned local Users" column shows ":: none ::". The "Assigned Network Blocks" column has a dropdown menu with the following options: "Any", "Internal (Address)", "Internal (Broadcast)", "Internal (Network)", and "Marketing" (which is selected). Below the dropdown are "Save" and "Cancel" buttons.

	△		Profile Name	Assigned local Users	Assigned Network Blocks
	1		Example	:: none ::	<div>Any Internal (Address) Internal (Broadcast) Internal (Network) Marketing</div> <div>Save Cancel</div>

The functions from the left to the right are:

Deleting Profile assignments (): Click the trash can icon to delete an assignment from the table.

Position number: The workout sequence will be displayed in the table through the respective **Position number**.

Clicking on the field with the entry will open the drop-down menu. This drop-down menu allows you, to change the order of the profile assignments. Save your changes by clicking on the **Save** button. To keep an entry, click **cancel**.

Status light: The status light refers to the status of the profile assignment: Each new assignment is not yet enabled (status light is red).

The profile assignment will be enabled by clicking on the status light (status light is green).

Profile Name: Select the **Surf Protection Profile** in this field from the Profiles Table.

Clicking on the field with the entry opens the drop-down menu. Save your changes by clicking on the **Save** button. To keep an entry, click **cancel**.

Assigned local Users: Select the **local user** from this field.

Clicking on this field with the entry opens the selection field. Save your changes by clicking on the **Save** button. To keep an entry, click **cancel**.

Important Note:

If you are simultaneously assigning a **Profile** to a **local user** and to a **network**, this *Profile* will only take effect, if the user accesses the HTTP proxy from the "configured" network! Only one **Surf Protection Profile** can be configured for each user or network.

Assigned Network Blocks: Select the **Network** from this field. Clicking on this field with the entry opens the selection field. Save your changes by clicking on the **Save** button. To keep an entry, click **cancel**.

Assigning Surf Protection Profiles:

By default, the table contains already a **Blank Assignment**. If this blank assignment has not been edited yet, continue with step 1.

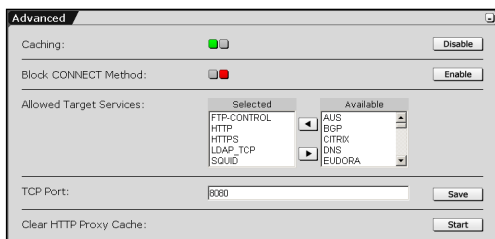
1. By clicking on the **Add blank Assignment** button, add a new blank assignment.
2. From the **Profile Name** field, select the **Surf Protection Profile**.
3. From the **Assigned local Users** field, select the local user for this profile.
4. From the **Assigned Network Blocks**, select the network for this profile.
5. Enable the profile assignment by clicking the **status light**.

The status light is green.

If a user or computer defined in the profile attempts to access a blocked website, access will be blocked, and the user will receive a message explaining why.

Using the Security System

Advanced



Caching: This function buffers often-used Websites to the **HTTP Proxy Cache**. This is enabled by default (status light shows green). Clicking on the **Disable** button disables this function.

Block CONNECT Method: All HTTP-connection requests will be blocked by the HTTP-proxy. Only the HTTP-methods **GET** and **PUT** will be allowed through the proxy.

Each Client Request will be introduced through the information of the method. Methods define the respective action for requests. The current HTTP-specification offers eight methods: OPTIONS, GET, HEAD, POST, PUT, DELETE, TRACE and CONNECT. Only the *GET* and *PUT* methods are explained in this section.

The **GET** method is used with requests from a document or another source. A source in this case is defined through the request-URL. There are two types: Conditional GET and partial GET. With the conditional-GET-type the request of data depends on certain conditions. The detail of these conditions is stored in the header-field Conditional. Often used conditions are for example If-Modified-Since, If-Unmodified-Since or If-Match. This condition helps to considerably reduce network utilization, since only the necessary data are forwarded. In practice, proxy servers, for example, use this function to prevent that data that are already stored in cache are forwarded several times. Also the partial GET-method has the same purpose. It uses the range-header-field that only forwards parts of the data, which, however, cannot be processed by the client yet. This technique is used for the resumption of an interrupted data transfer.

The **PUT** method allows for a modification of existing sources and/or for the creation of new data on the server. In contrast to the POST-

method, the URL in the PUT-request identifies the data sent with the request and not the source.

Clicking on the **Enable** button enables the function (status light is green).

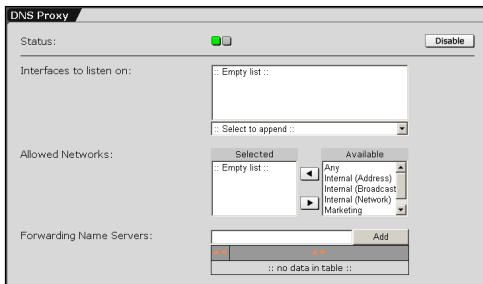
Allowed Target Services: Use the **Allowed target services** selection menu to choose services that the HTTP proxy should be allowed to access. By default, the services with the ports are already available, to which a connection is considered as being safe.

TCP Port: Enter the **TCP/IP-Port** in the entry field. By default, this is set to the TCP/IP-Port **8080**.

Clear HTTP Proxy Cache: The **HTTP Proxy Cache** proxy stores a copy of often-visited pages locally, reducing load times.

By clicking the **Start** button, the cache will be cleared, and any new accesses will be loaded from the remote Internet site.

5.6.2. DNS



The **DNS Proxy** service allows you to provide internal clients with a secure and efficient **name server** service. If you select multiple remote name servers, they will be queried in the order they are entered.

The DNS entries in network definitions are resolved every minute by the DNS Resolver. If now a DNS entry refers to a Round-Robin-DNS, the definition can be actualized every minute. The Round-Robin-DNS process offers an easy opportunity to distribute user requests to individual servers, such as to a server farm. With the Round-Robin-DNS, the IP addresses of all servers of the server farm are assigned to a hostname in the *Domain Name Service (DNS)*. If clients now

Using the Security System

request the IP address of this hostname there, the DNS sequentially reports these IP addresses back. Thus, a distribution of the client requests to the respective servers is achieved.

The disadvantage of the Round-Robin process is that neither a failure nor the utilization of the individual servers is accounted for.

If no name servers are entered in the **Forwarding Name Servers** menu, the proxy will use the Internet-wide ROOT name servers. If you or your ISP runs a name server that is closer, you should enter its IP address here. This means, however, that they are usually slower than closer name servers.

The ROOT name servers are an integral part of the Internet. 15 ROOT name servers are distributed worldwide and are the basic instance for all secondary name servers.

Tip:

Even if you do not plan to use the DNS proxy, you should enter the address of your provider's DNS server address as a forwarding server. Those will be used by the firewall itself, even if the proxy is disabled. This contributes to the discharge of the root name server and the firewall produces only local queries, which generally receive faster replies.

Configuring the DNS Proxy:

1. In the **Proxies** tab, open the **DNS** menu.
2. Click the **Enable** button to start the proxy.
Another entry window will open.
3. Make the following settings:

A description of how to use the **selection field** tool can be found in chapter 4.3.2 on page 36.

Interfaces to listen on: Select which network cards the DNS proxy server should be reachable on. This should usually only be

the internal network cards.

Network cards are configured in the **Network/Interfaces** menu. Further information is available in chapter 5.3.2 on page 119.

Allowed Networks: Select which networks should have access to the proxy server.



Security Note:

In the **Allowed networks** menu, do not select **Any** unless absolutely necessary. If **any** is selected, the **DNS Proxy** can be used by any Internet user.

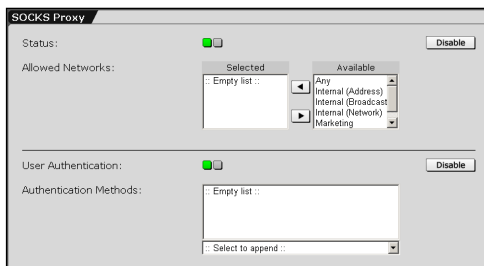
Forwarding Name Servers: Enter the IP addresses of your name server here.

Click **Add** to add each name server to the list.

Ordered Lists are described in chapter 4.3.4 on page 39.

All settings take effect immediately and will be saved if you leave this menu.

5.6.3. SOCKS



SOCKS is a generic proxy, used by many client applications. Examples include Instant Messaging Clients such as ICQ or AIM, FTP clients, and RealAudio. SOCKS can build TCP connections for client applications, and can

also provide incoming (listening) TCP and UDP ports. This is especially important for systems using NAT, as SOCKS mitigates the drawbacks of having all internal clients use the same external address. This security system supports the protocols SOCKSv4 and SOCKSv5.

Using the Security System

Please note, however, that the SOCKSv4 protocol does not support **User Authentication**.

Note:

If you wish to use SOCKSv5 with name resolution, you must also activate the DNS proxy service.

Configuring the SOCKS Proxy:

1. In the **Proxies** tab, open the **SOCKS** menu.
2. Click the **Enable** button next to **Status** to start the proxy.
Another entry window will open.
3. Make the following settings:

A description of how to use the **selection field** tool can be found in chapter 4.3.2 on page 36.

Allowed Networks: Here you can select the networks and hosts that should be allowed to use the proxy.

All settings take effect immediately and will be saved if you leave this menu.

SOCKS-Proxy with User Authentication:

If you have enabled the **User Authentication** function, proxy users must use a username and password to log into the SOCKS proxy. Because only SOCKSv5 supports **User Authentication**, SOCKSv4 is automatically disabled.

The **Authentication Methods** selection menu allows you to select the user authentication method to be used. Only those authentication methods, you have configured in the **Settings/User Authentication** menu are available here. If you choose to use the **Local Users** method, you can select which local users may access the **SOCKS**

Using the Security System

Proxy.

Local **Users** are managed in the **Definitions/Users** menu.

Using the Security System

5.6.4. POP3

The screenshot shows the 'Transparent POP3 Proxy' configuration window. It has a 'Status' section with a green indicator and a 'Disable' button. Below is the 'Proxied networks' section with 'Source' and 'Destination' dropdown menus (both set to 'Please select...') and an 'Add' button. A table titled 'Configured Proxied Networks' shows a single entry with 'Source' as 'Any' and 'Destination' as 'Any', with a 'delete' action button. The 'Content Filter' section includes 'Virus Protection' and 'Spam Protection' (both with red indicators and 'Enable' buttons), and 'File Extension Filter' and 'Expression Filter' (each with a text input, an 'Add' button, and a table showing no data).

POP3 stands for **Post Office Protocol 3**: This is a protocol, which allows the retrieval of e-mails from a mail server. POP3 is the logical opposite of **SMTP**. SMTP stands for Simple Mail Transfer Protocol. This protocol is used to deliver e-mails to a mail server.

This menu allows you to configure the **POP3 Proxy** for incoming e-mails. The POP3 proxy works transparently, requiring no configuration on the client side. POP3 requests coming from the internal network on port 110 are intercepted and redirected through the proxy. This process is not visible to the client. The advantage of this mode is that no additional administration or configuration is required on the client of the end user.

Configuring the POP3 Proxy:

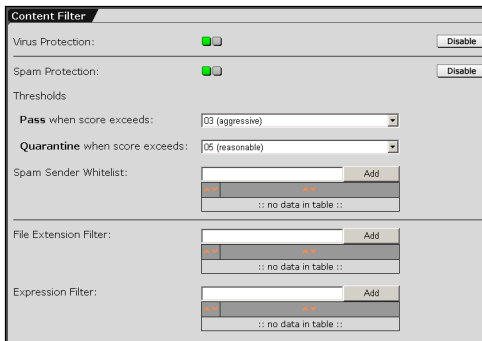
Normally, the POP3 proxy must only be enabled in order to process POP3 requests, as it proxies for all networks by default. The **Configured Proxied Networks** displays which networks are to be allowed.

If only POP3 requests from certain networks should be forwarded, the configuration must be changed. Note that the drop-down menus contain only those networks you have already defined in the **Definitions/Networks** menu.

Example: POP3 queries from the subnet 192.168.0.0/ 255.255.0.0 to pop.yoursite.com should be forwarded through the proxy. These networks must first be defined in the **Networks** menu. Once this is done, continue as follows:

1. In the **Proxies** tab, open the **POP3** menu.
2. Click the **Enable** button next to **Status** to start the proxy.
An advanced entry window will open.
3. In the **Proxied Networks** window, choose the networks that the proxy should intercept requests from and to.
Source: Choose the source address here.
Example: The name of the 192.168.0.0/255.255.0.0 network.
Destination: Choose the destination address here.
Example: The name of the pop.yoursite.com network.
4. Confirm your selection by clicking **Add**.

Content Filter



Content Filter

Virus Protection: ☐ **Disable**

Spam Protection: ☐ **Disable**

Thresholds

Pass when score exceeds: 03 (aggressive)

Quarantine when score exceeds: 05 (reasonable)

Spam Sender Whitelist:

IP	Score
:: no data in table ::	

File Extension Filter:

File Extension	Score
:: no data in table ::	

Expression Filter:

Expression	Score
:: no data in table ::	

Virus Protection: This option scans e-mails and attachments passing through the proxy for dangerous contents such as viruses or Trojan horses. The results of the scan are inserted into a header of the message. Any messages blocked by the proxy will be shown in the

Proxies/Proxy Content Manager menu. Enable the **Virus Protection** by clicking on the **Enable** button (status light is green).

Spam Protection: This option heuristically checks incoming e-mail for characteristics suggestive of spam. This system uses an internal database of heuristic tests and characteristics, making the test independent from sender information, and also more reliable.

Two **Thresholds** can be defined for the Spam Score. This ensures that potential SPAM e-mails are treated differently by the Firewall.

Using the Security System

Default settings:

Thresholds

Pass when Score exceeds: 03 (aggressive)

Quarantine when Score exceeds: 05 (reasonable)

The first threshold implicates that e-mails from level 3 on are filtered, but allowed through. With the help of the attached Header the e-mail on the mail-server or in the e-mail-program of the recipient can be sorted or filtered. For the second threshold the e-mail will be accepted but put into quarantine.

Basically, the **Threshold** with the higher level is treated more severely.

Important Note:

On busy systems, the **Spam Protection** may require a large percentage of system resources.

Pass/Quarantine when Score exceeds: These drop-down menus can be used to select the strategy to use in marking messages as spam. The difference between the maximum values is defined through the probability that legitimates messages, such as HTML Newsletters will be blocked. It is possible to set a value between 1 and 15 in the drop-down menu. With level 1, the e-mails are already treated with a low spam score. The following Levels serve as clue:

- **Aggressive (03):** This strategy will catch most spam messages. It may also identify some legitimate messages, for example HTML newsletters, as spam.
- **Reasonable (05):** This strategy is a compromise between **Aggressive** and **Reasonable**
- **Conservative (08):** This strategy will only catch messages that are highly likely to be spam. Legitimate messages are unlikely to be caught.

The following actions are preset:

- **Quarantine:** The e-mail will be accepted, but kept in quarantine. The **Proxy Content Manager** menu will list this e-mail with status **Quarantine**. This menu presents further options, including options to read or to send the message.
- **Pass:** The proxy will add a **Header** to the message noting that it has found a potentially dangerous string, but will then allow the message to pass. A **Header** will be added to the e-mail, by which it can be sorted or filtered on the mail server or in the e-mail program of the recipient. In addition, the word ***SPAM*** will be added to the message subject line.

For a description of how to create rules in **Microsoft Outlook 2000** please see on page 252.

The Header:

Many of the SMTP proxy functions will add **headers** to the messages scanned. The Header will inform the user on specific characteristics of a message. If you select the **Pass** action, recipients can configure their e-mail programs to filter messages with high spam scores.

The following list contains all possible *Headers*:

- **X-Spam-Score:** This header is added by the **Spam Detection** module. It contains a score, consisting of a numerical value and of a number of minus and plus characters. The higher the value, the more likely it is that the message is spam.
If you select the **Pass** action under **Spam Protection**, recipients can configure their e-mail programs to filter messages with high spam scores.
- **X-Spam-Flag:** This header is set to **Yes** when the proxy classifies a message as spam.

Using the Security System

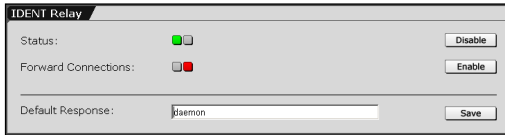
- **X-Spam-Report:** The proxy identified a message as spam. The added Multiline Header contains a readable and accessible anti-spam report.

Spam Sender Whitelist: This control list can only be defined for the **Spam Protection** option. Enter the e-mail addresses of those senders into the list, whose messages you wish to allow through.

File Extension Filter: The firewall filters attachments with the extensions from the control list.

Expressions Filter: This function allows to filter all e-mail texts and attached text files, that pass through the POP3 proxy by specific expressions. The expressions are defined in the check list in the form of **Perl Compatible Regular Expressions**.

5.6.5. Ident



The **Ident** protocol allows external servers to associate a username with given TCP connections.

While this connection is not encrypted, it is nevertheless necessary for many **services**.

If you enable the **Ident** function, the security system supports Ident queries. The system will always reply with the string that you define as **Default Response**, irrespective from which local service the connection will be started.

Forward Connections: Ident queries cannot be answered through **Connection Tracking**. You can get around this difficulty if you use the **Masquerading** function: in that case, the **Forward Connection** function will pass the ident request on to the internal **masquerading** host.

Please note, however, that the actual (internal) IP address will not be released. Instead, the system will query the internal machine, and simply pass the response string to the remote server. This is often useful for internal clients with a mini-ident server, such as the ones often included in IRC and FTP clients.

Using the Security System

5.6.6. SMTP

The screenshot displays the SMTP configuration window with three tabs: Global Settings, Incoming Mail, and Outgoing Mail.

Global Settings:

- Status: ☒ (Disable button)
- Hostname (MX):
- Postmaster Address:
- Max Message Size:
- DoS Protection: ☒ (Disable button)
- Save button

Incoming Mail:

- Domain Name:
- SMTP Host: (Add button)
- SMTP Routes Table:

Domain Name	SMTP Host	Actions
no SMTP routes defined		
- Recipient Verification: ☒ (Enable button)

Outgoing Mail:

- Allowed Networks: Selected (Empty list) and Available (Any Internal (Address), Internal (Broadcast), Internal (Network), Marketing) lists with arrows between them.
- Use Smarthost: ☒ (Enable button)

An **SMTP Proxy** allows you to protect an internal mail server from remote attacks. While forwarding and receiving messages, the proxy can also scan them for potentially dangerous contents. This menu also allows you to configure anti-spam parameters in order to block unwanted e-mails.

This menu allows you to configure the **POP3 Proxy**

for incoming e-mails. The **SMTP Proxy** receives all e-mails at the gateway and then forwards them to their destination. Because there is no direct contact between internal and external machines, only data is transferred, and no protocol errors will propagate. The SMTP proxy monitors the SMTP protocol on TCP port 25.

Note:

In order to use the **SMTP Proxy** correctly, a valid **name server (DNS)** must be activated. System notifications are sent to the administrator even if the **SMTP proxy** is disabled.

Configuring the SMTP Proxy:

1. In the **Proxies** tab, open the **SMTP** menu.
2. Click the **Enable** button next to **Status** to start the proxy.
3. In the **Global Settings** window, configure the basic settings.

Hostname (MX): Enter the hostname here.

Important Note:

If you wish to use TLS encryption, this hostname must be identical with the one listed in your DNS server's **MX record**. Otherwise, other mail servers using TLS will refuse to send incoming mails.

Postmaster Address: Enter the e-Mail address of the postmaster here.

Max message size: Enter the maximum message size for in- and out-bound mail messages. Normal values are 20 or 40 MB. Please note that the encoding used to transmit e-mails can make the size of the message larger than the files sent.

4. Save your settings by clicking **Save**.
5. Enable the **DoS Protection** by clicking the **Enable** button.

In order to protect the security system against a **Denial of Service (DoS)** attack, a maximum of 25 incoming concurrent connections are supported. The 26th connection will not be accepted.

By default, the **DoS Protection** function is enabled.

6. In the **Incoming Mail** window, set the route for incoming mails.

Domain Name: In order to send mails for a certain domain to the correct machine, the domain name (e.g., mydomain.com) must be configured here.

SMTP Host: All e-mails for this domain can be forwarded to a certain host. This will normally be a host like **Microsoft**

Using the Security System

Exchange Server or **Lotus Notes**. The host must be defined in the **Definitions/Networks** before it will appear in the drop-down menu.

You can also set the system to forward e-mails to the system specified by the MX record. You should take care that the firewall itself is not the MX host for the domain.

7. Confirm your selection by clicking **Add**.

Recipient Verification: The SMTP proxy will only accept incoming e-mails after verifying that the receiving address exists. This will dramatically reduce the number of spam messages received, as only messages with valid destination addresses will be accepted.

This function requires that the internal SMTP server reject messages to unknown addresses. The basic rule: The basic rule is that if the mail server rejects a message, then so too will the firewall.

8. In the **Outgoing Mail** window, select the **Allowed Networks** or hosts to which outgoing mail should be proxied.



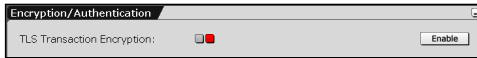
Security Note:

Messages sent from those networks will never be scanned by **Spam Detection**.

Use Smarthost: If you wish to use an **Upstream Smarthost** to deliver messages, enable this function and enter the IP address of the smarthost here. In this case, the proxy will not attempt to deliver messages itself, but will instead forward them to the smarthost. The proxy will, however, deliver messages locally to domains defined in the **Incoming Mail** window.

For the Smarthost the **Username** and **Password** can optionally be defined.

Encryption/Authentication



The **TLS Transaction Encryption** function allows you to automatically encrypt in- and out-going e-mails at the transport layer. You must first confirm that the remote host supports this function. TLS is used for encryption, not just authentication. SMTP is generally not encrypted and can easily be read by third persons. The function should therefore be enabled.

Important Note:

Some mail servers, such as Lotus Domino, use non-standard implementations of **TLS**. While these servers claim to support TLS during connection negotiation, they cannot establish a TLS full session. If TLS is enabled, it will not be possible to send messages to these servers. In such situations, please contact the administrator of the mail server.

If the **TLS Transaction Encryption** function is activated, you can also use **SMTP Authentication**. This allows mail clients such as Microsoft Outlook, Outlook Express, or Netscape Messenger to authenticate themselves to the **SMTP Proxy**. This is especially useful for clients with dynamic IP addresses, where the client IP address cannot be specified in the **Outgoing Mail** menu.

When configuring clients, please note that SPA (Secure Password Authentication) should not be used. SPA is an alternative encryption method, which is not supported by this security system. You should use an unencrypted authentication method instead, and use TLS (or SSL) to encrypt the session.

The **Authentication Methods** selection field allows you to select the user authentication method to be used. Only those authentication methods you have configured in the **Settings/User Authentication** menu are available here.

Local users are defined in the **Definitions/Users** menu.

Using the Security System

Global Whitelist



Trusted Hosts/Networks:

In the hierarchy list a **Global Whitelist** can be defined with reliable hosts or networks, which in this

case are excluded from the following options:

- Realtime Blackhole Lists
- Sender Verification
- MIME Error Checking
- Spam Detection
- Expression Filter

This implicates, that the necessary computing power for scans is reduced and that problematic hosts can be excluded from Content Scanning.

Trusted Domains: In the ordered list a Global Whitelist can be defined with a reliable Domain name.



Security Note:

This function should only be used carefully, since sender addresses can easily be falsified.

5.6.6.1. Virus Protection/Content Filter

Block RCPT Hacks

When this function is enabled, the proxy will reject e-mails with a sender address containing the characters **!**, **%**, **/**, or **|**. In addition, addresses with an extra **@** symbol, or which begin with a **dot** (.) will also be blocked.

Sender Blacklist

This function allows you to create a list of sender addresses, for example those of known spam senders. The proxy will then reject all messages with these addresses in either the From or Reply-To headers.

Enter the e-mail addresses according to the following description into the **Patterns** control list:

- To block e-mails from a certain address.
Entry: user@domain.com
- To block all e-mails from a certain domain.
Example: *@domain.com
- To block all e-mails from a certain user, no matter what domain is used to send the message.
Example: user@*

The function of the **Control List** is identical to the **Ordered List** and described in chapter 4.3.4 on page 39.

If the firewall receives an e-mail from a blocked address, a **5xx** error code will be issued with the message **Your address (envelope or header) is blacklisted at this site.**

Using the Security System

MIME Error Checking

The **MIME Error Checking** module can detect errors in messages that have been encrypted with **MIME**. **MIME** stands for **M**ultipurpose **I**nternet **M**ail **E**xtensions. MIME defines the structure and the composition of e-mails and of other Internet messages. This is an encoding rule, which allows for the transmission of non-text documents, e.g. pictures, audio and video in text based transmission systems. The non-text elements are encrypted at the sender and decrypted at the receiver.

The **MIME Error Checking** module can help detecting attacks, in which error tolerance variations in the MIME-decryption-software are being utilized.

Action: This drop-down menu allows you to select the action the proxy should take upon finding a message with a filtered string. The following actions are possible:

- **Reject:** The message will be bounced back to the sender with a **5xx** error message. The bounce message sent to the sender will also contain an explanation of why the message was blocked.
- **Blackhole:** The e-mail will be accepted and silently dropped. Do not use this action unless you are absolutely certain no legitimate e-mails will be lost.
- **Quarantine:** The e-mail will be accepted, but kept in quarantine. The **Proxy Content Manager** menu will list this e-mail with status **Quarantine**. This menu presents further options, including options to read or to send the message.
- **Pass:** The e-mail will be treated by the filter, but allowed to pass. A **Header** will be added to the e-mail, by which it can be sorted or filtered on the mail server or in the e-mail programs of the recipient.

For a description of how to create rules in **Microsoft Outlook 2000** please see on page 252.

Trigger on: In this drop-down menu you define, which errors cause, that the e-mail is treated according to the Action function:

- **Level 1:** This step causes, that only e-mails with most serious errors are treated. This setting is recommended, since many users use a deficient encryption program, that already responds in the higher levels (Level 2 und 3).
- **Level 2:** With the exception of the e-mails with the ordinary errors, all are being treated.
- **Level 3:** Any e-mails with errors are being treated.

File Extension Filter

This module allows the firewall to selectively filter attachments based on their file extensions. The extensions to filter can be selected in the **Extensions** list tool.

Action: This drop-down menu allows you to select the action the proxy should take upon finding a message with a filtered string. The following actions are possible:

- **Reject:** The message will be bounced back to the sender with a **5xx** error message. The bounce message sent to the sender will also contain an explanation of why the message was blocked.
- **Blackhole:** The e-mail will be accepted and silently dropped. Do not use this action unless you are absolutely certain no legitimate e-mails will be lost.
- **Quarantine:** The e-mail will be accepted, but kept in quarantine. The **Proxy Content Manager** menu will list this e-mail with status **Quarantine**. This menu presents further options, including options to read or to send the message.
- **Pass:** The e-mail will be treated by the filter, but allowed to pass. A **Header** will be added to the e-mail, by which it can be sorted or

Using the Security System

filtered on the mail server or in the e-Mail programs of the recipient.

For a description of how to create rules in **Microsoft Outlook 2000** please see on page 252.

Extensions: Enter the file extensions (e.g. **exe**), that the firewall should filter.

The function of the **Control List** is identical to the **Ordered List** and described in chapter 4.3.4 on page 39.

Virus Protection

The **Virus Protection** function allows you to check e-mails and attachments for dangerous contents such as viruses, Trojan horses, and so on. The results of the scan are inserted into a header of the message.

If the **Virus Protection** discovers an infected e-Mail, the message will be filtered by the firewall. The further handling will be according to the setting configured in the **Action** drop-down menu.

Action: This drop-down menu allows you to select the action the proxy should take upon finding a message with a filtered string. The following actions are possible:

- **Reject:** The message will be bounced back to the sender with a **5xx** error message. The bounce message sent to the sender will also contain an explanation of why the message was blocked.
- **Blackhole:** The e-mail will be accepted and silently dropped.
- **Quarantine:** The e-mail will be accepted, but kept in quarantine. The **Proxy Content Manager** menu will list this e-mail with status **Quarantine**. This menu presents further options, including options to safely read the message.
- **Pass:** The e-mail will be treated by the filter, but allowed to pass. A **Header** will be added to the e-mail, by which it can be sorted or

filtered on the mail server or in the e-mail programs of the recipient.

For a description of how to create rules in **Microsoft Outlook 2000** please see on page 252.

Expression Filter

There is the chance that new viruses will appear which are not yet recognized by the firewall. Various viruses can be identified because of known strings – such as the IloveYou virus. The strings are entered into this module. If an e-mail contains this string, it will be blocked.

Next to simple strings, also expressions in the form of **Perl Compatible Regular Expressions** can be defined.

Action: This drop-down menu allows you to select the action the proxy should take upon finding a message with a filtered string. The following actions are possible:

- **Reject:** The message will be bounced back to the sender with a **5xx** error message. The bounce message sent to the sender will also contain an explanation of why the message was blocked.
- **Blackhole:** The e-mail will be accepted and silently dropped.
- **Quarantine:** The e-mail will be accepted, but kept in quarantine. The **Proxy Content Manager** menu will list this e-mail with status **Quarantine**. This menu presents further options, including options to read or to send the message.
- **Pass:** The e-mail will be treated by the filter, but allowed to pass. A **Header** will be added to the e-mail, by which it can be sorted or filtered on the mail server or in the e-mail programs of the recipient.

For a description of how to create rules in **Microsoft Outlook 2000** please see on page 252.

Expressions: Enter the strings to filter in this list.

Using the Security System

The function of the **Control List** is identical to the **Ordered List** and described in chapter 4.3.4 on page 39.

5.6.6.2. Spam Protection

Sender Address Verification

When this function is enabled, the sending address of incoming e-mails will be checked. And also sending domain will be checked. If the sending domain does not exist, the e-mail will be rejected.

If the **Callout** function is also enabled, the proxy will connect to the mail server of the sending domain and check the sender address using an RCPT command. If the sending address does not exist, the proxy will reject messages from it.

Realtime Blackhole Lists (RBL)

The **RBL** module uses an external database of known spam senders to check sending addresses. Several services of this type are available on the Internet. This function helps to massively reduce the number of spam.

One commercial service, for example, can be found at <http://www.mail-abuse.org>.

Action: This drop-down menu allows you to define how filtered e-mails originating from known spam-sending domains should be handled. The following actions are possible:

- **Warn:** If an e-mail is received from an RBL-listed domain, the **X-RBL-Warning** header will be inserted in the message, and the message will be allowed to pass through the proxy. More information on inserted headers can be found in the **Spam Detection** section.
- **Reject:** E-mails from listed domains will not be accepted, and will instead be bounced back to the sender.

Zone: Enter the addresses of databases to use in this list.

The function of the **Control List** is identical to the **Ordered List** and described in chapter 4.3.4 on page 39.

Spam Protection

This option heuristically checks incoming e-mail for characteristics suggestive of spam. This system uses an internal database of heuristic tests and characteristics, making the test independent from sender information, and also more reliable.

Two **Thresholds** can be defined for the Spam Score. This ensures that potential SPAM e-mails are treated differently by the Firewall.

The two **Thresholds** are equal. Whereas the threshold with the higher level should be treated more severely. The functioning is explained below with the help of the default settings.

Default settings:

Threshold One

When Spam Level exceeds: 03 (aggressive),
do this: Pass.

Threshold Two

When Spam Level exceeds: 05 (reasonable),
do this: Quarantine.

The first threshold implicates that e-mails from level 3 on are filtered, but allowed through. With the help of the attached Header the e-mail on the mail-server or in the e-mail-program of the recipient can be sorted or filtered.

For the second threshold the e-mail will be accepted but put into quarantine.

Basically, the **Threshold** with the higher level is treated more severely (**do this**).

Using the Security System

Important Note:

On busy systems, the **Spam Detection** may require a large percentage of system resources.

When Spam Level exceeds: This drop-down menu can be used to select the strategy to use in marking messages as spam. The difference between the maximum values is defined through the probability that legitimates messages, such as HTML Newsletters will be blocked. It is possible to set a value between 1 and 15 in the drop-down menu. With level 1, the e-mails are already treated with a low spam score. The following Levels serve as clue:

- **Aggressive (03):** This strategy will catch most spam messages. It may also identify some legitimate messages, for example HTML newsletters, as spam.
- **Reasonable (05):** This strategy is a compromise between **Aggressive** and **Reasonable**
- **Conservative (08):** This strategy will only catch messages that are highly likely to be spam. Legitimate messages are unlikely to be caught.

do this: This drop-down menu allows you to select the action the proxy should take upon finding a message with a filtered string. The following actions are possible:

- **Reject:** The message will be bounced back to the sender with a **5xx** error message. The bounce message sent to the sender will also contain an explanation of why the message was blocked.
- **Blackhole:** The e-mail will be accepted and silently dropped. Do not use this action unless you are absolutely certain no legitimate e-mails will be lost.
- **Quarantine:** The e-mail will be accepted, but kept in quarantine. The **Proxy Content Manager** menu will list this e-mail with status

Quarantine. This menu presents further options, including options to read or to send the message.

- **Pass:** The e-mail will be treated by the filter, but allowed to pass. A **Header** will be added to the e-mail, by which it can be sorted or filtered on the mail server or in the e-Mail programs of the recipient. In addition, the word ***SPAM*** will be added to the message subject line.

For a description of how to create rules in **Microsoft Outlook 2000** please see on page 252.

Spam Sender Whitelist: This control list is defined for the **Spam Protection** function. Enter the e-mail addresses of those senders into the list, whose messages you wish to allow through.

The function of the **Control List** is identical to the **Ordered List** and described in chapter 4.3.4 on page 39.

The Header:

Many of the functions will add **headers** to the messages scanned: The Header will inform the user on specific characteristics of a message. If you select the **Pass** action, recipients can configure their e-mail programs to filter messages with high spam scores. The following is a list of the headers the SMTP proxy may insert:

- **X-Spam-Score:** This header will be added to the **Spam Detection** module. It contains a score, consisting of a numerical value and of a number of minus and plus characters. The higher the value, the more likely it is that the message is spam.
If you select the **Pass** action under **Spam Detection**, recipients can configure their e-mail programs to filter messages with high spam scores.
- **X-Spam-Flag:** This header is set to **Yes** when the proxy classifies a message as spam.

Using the Security System

- **X-Spam-Report:** The proxy identified a message as spam. The added Multiline Header contains a readable and accessible anti-spam report.
- **X-Infected:** This header is added if a virus is detected within the message. The value of the header is the name of the virus found.
- **X-Contains-File:** When the **File Extension Filter** is enabled and an attachment with a potentially dangerous extension is found, the proxy will add this header.
- **X-Regex-Match:** When the **Expression Filter** is enabled and an attachment matching the configured regular expression is found, the proxy will add this header.
- **X-RBL-Warning:** When the **Realtime Blackhole Lists (RBL)** function is enabled and the sending domain is listed in the **Zones** list, this header will be added. Note that this header will only be added if the RBL system is configured to **Warn**.

Creating rules in Microsoft Outlook 2000:

MS Outlook allows you to sort those e-mails, which had been filtered and subsequently been allowed to pass through the Firewall, provided that the **Pass** function in the **Action** drop down menu of the corresponding modules on the Firewall has been selected.

1. Start **MS Outlook**.
2. Click on **Inbox**.
3. Open the menu **Tools/Rules Wizard**.
4. Click on the button **New**.

The Rules Wizard opens, in order to set new rules. The Rules wizard now leads you step-by-step through the configuration.

5. Which type of rule do you want to create? (step 1)
Select the rule **Check messages when they arrive**.

Then click on the button **Next**.

6. Which condition(s) do you want to check? (step 2)

In this window, select the condition **with specific words in the message header**.

In the window **Rule description** click on the underlined portion of text and type the header's name into the input field **Search text**.

Example: **X-Spam-Score**

Then click on the button **Next**.

7. What do you want to do with message? (step 3)

Define in this window, what has to be done with the filtered e-mail. If for instance, you want to move the filtered e-mails to a specific folder, select the action **move it to a specified folder**.

With one click on **Specified folder** in the window **Rule description**, a new menu appears. Here you can either choose an existing folder or create a new destination folder for the filtered e-mails. Example: **Spam**

Click **OK** to save the new settings in this menu.

Then click on the button **Next**.

8. Add exceptions (step 4)

The module **Spam Detection** heuristically checks incoming e-mails for certain characteristics. It therefore might be, that safe messages, e.g. HTML-Newsletter are filtered. This menu allows you to define exceptions and to thus exclude e-mails, e.g. messages of a particular sender from this rule.

Then click on the button **Next**.

9. Enter a name for this rule (step 5)

Type a distinct name for this rule into the input field. In the options fields below, you can **activate** these rules and also apply them on e-mails, which are already in the **Inbox** folder. You can change your settings in the window Rule description.

Using the Security System

Then click on the button **Finish**.

10. Apply rules in the following order (step 6)

In the Rules Wizard you can activate or deactivate the rules by one click on the option field or execute changes.

In order to close the Rules Wizard, click on the button **OK**.

5.6.7. Proxy Content Manager

The **Proxy Content Manager** menu allows you to manage all of the e-mails quarantined by the proxy, as well as those which, because of an error, the system was unable to forward.

This menu uses the following concepts to display and manage the e-mails:

Global Actions

Please select:

Refresh proxy content table

Start

SMTP / POP3 proxy content

Total 17 entries

Filters

	Type	Age		Sender	Recipient(s)
<input type="checkbox"/>	POP3	4h 10m	✘ SP	<rdiehl@vinet.qa>	rdiehl@vinet.qa
<input type="checkbox"/>	SMTP	2d 23h 34m	✘ EXP	<rdiehl@vinet.qa>	✘ rdiehl@vinet.qa
<input type="checkbox"/>	SMTP	2d 23h 36m	✘ EXP	<rdiehl@vinet.qa>	✘ rdiehl@vinet.qa
<input type="checkbox"/>	POP3	3d 0h 4m	✘ VP	<rdiehl@vinet.qa>	rdiehl@vinet.qa
<input type="checkbox"/>	POP3	3d 1h 7m	✘ SP	<rdiehl@vinet.qa>	rdiehl@vinet.qa
<input type="checkbox"/>	POP3	3d 1h 9m	✘ SP	<rdiehl@vinet.qa>	rdiehl@vinet.qa
<input type="checkbox"/>	POP3	3d 1h 10m	✘ VP	<rdiehl@vinet.qa>	rdiehl@vinet.qa
<input type="checkbox"/>	POP3	3d 1h 11m	✘ VP	<rdiehl@vinet.qa>	rdiehl@vinet.qa
<input type="checkbox"/>	SMTP	3d 1h 20m	✘ SP	<rdiehl@vinet.qa>	✘ rdiehl@vinet.qa
<input type="checkbox"/>	SMTP	3d 1h 37m	✘ VP	<rdiehl@vinet.qa>	✘ rdiehl@vinet.qa
<input type="checkbox"/>	SMTP	3d 1h 46m	✘ FILE	<rdiehl@vinet.qa>	✘ rdiehl@vinet.qa
<input type="checkbox"/>	SMTP	3d 2h 8m	✘ VP	<rdiehl@vinet.qa>	✘ rdiehl@vinet.qa
<input type="checkbox"/>	SMTP	3d 2h 10m	✘ VP	<rdiehl@vinet.qa>	✘ rdiehl@vinet.qa
<input type="checkbox"/>	POP3	3d 2h 11m	✘ VP	<rdiehl@vinet.qa>	rdiehl@vinet.qa
<input type="checkbox"/>	SMTP	3d 2h 16m	✘ VP	<rdiehl@vinet.qa>	✘ rdiehl@vinet.qa
<input type="checkbox"/>	SMTP	3d 2h 17m	✘ VP	<rdiehl@vinet.qa>	✘ rdiehl@vinet.qa
<input type="checkbox"/>	SMTP	3d 3h 24m	✘	<>	✘ do-not-reply@fw-notify.net

checked entries: Please select:

ID: Every e-mail in this security system contains a unique **ID**. This **ID** is contained in the header of the message, and is used by the system to identify messages in the log files. The **ID** will be displayed, when you touch the entry in the **Type** field with the mouse.


Type: Proxy Content Manager distinguishes between the **POP3** and **SMTP** types of filtered e-mail: If you touch the entry with the mouse, the **Mail-ID** will be displayed. Clicking on the entry opens a window with the content of the message. Thus you can safely read important

Using the Security System

messages. Messages of a length of up to 500 lines will be displayed completely.

Age: This column displays the age of an e-mail, i.e., the period of time since when the e-mail has arrived to the Internet security system.

Status: The states of the e-mails are displayed in the Proxy Content Manager through symbols.

- **deferred** (

On the right side, next to the status symbol for those e-mails, which are kept in quarantine, it is displayed which function blocked the message:

SP: Spam Protection

VP: Virus Protection

Filter: File Extension Filter



EXP: Expression Filter

MIME: MIME Error Checking

- **permanent error/andauernder Fehler** (

Sender: The sender of an e-mail is displayed in this column. For the *SMTP* type, this is the sender address on the envelope.

For the *POP3* type, this is the address of the „*From:*“-header of an e-mail. If no sender address is displayed, the e-mail contains the additional status **Bounce**.

Recipient(s): The recipient of an e-mail is displayed in this column. For the *SMTP* type, this is the recipient's address on the envelope. For e-mails with the **deferred** status, the delivery status will be displayed separately for each recipient: Deferred () or permanent error ()

The drop-down menu at the bottom of the table shows further functions to manage single e-mails. Click the selection box next to an e-mail to manage it.

The following functions are available:

Delete: All chosen e-mails will be deleted.

Force delivery: All chosen e-mails will be forwarded to the recipient addresses, even those having a **quarantined** status. For e-mails with a **deferred** or **permanent error** status, it is being tried again to deliver the message. If the system encounters another problem delivering it, the message will return to its previous status.

Download as .zip file: The chosen e-mails are packed into a zip-file and then saved to the selected local host.

Using the Security System

Global Actions

In order to save disk space on the security system, you can use this option to delete all messages of a certain type. E-mails being sent or forwarded while the system is deleting messages will not be affected. From the **Please select** drop-down menu, select the type and start the action by clicking on the **Start** button.

If you wish to actualize the **SMTP/POP3 Proxy Content** table, select the **Refresh proxy content table** action from the **Please select** drop-down menu.

Attention:

Messages of the selected type will be deleted without further confirmation.

Filters

The **Filters** function allows you to filter *E-Mails* with specific attributes from the table. The function facilitates the management of huge networks, since the protocols of a specific type can be presented in a concise way.

Filtering e-mails:

1. Click on the **Filters** button.

The entry window will open.

2. Enter the filter attributes in the following fields. Not all attributes have to be defined.

Type: If you wish to filter e-mails of a specific type, select them from the drop-down menu.

Status: If you wish to filter e-mails of a specific status, select them from the drop-down menu.

Using the Security System

Content Filter Type: This drop-down menu allows you to filter e-mails, that have been filtered by a specific function from the Content-Filter-Modules.

Sender: This drop-down menu allows you to filter e-mails with a specific sender address.

Recipient(s): This drop-down menu allows you to filter e-mails with a specific recipient address.

3. Click the **Apply Filters** button to start the filter.

In this case, only the filtered e-mails will be displayed in the table. Once the menu has been left, all protocols will be displayed again.

5.7. Virtual Private Networks (IPSec VPN)

A **Virtual Private Network (VPN)** is a secure connection between two networks over an untrusted network (such as the Internet).

VPNs are very useful when sensitive information must be transmitted or received over the Internet. The VPN prevents third parties from reading or modifying the information in transit. The connection is controlled and secured by the software installed at the connection endpoints. This software implements authentication, key exchange, and data encryption according to the open **Internet Protocol Security (IPSec)** standard.

Only authenticated computers can communicate through a **VPN**-protected connection. No other computer can transmit information over this connection.

VPN connections can be established between two hosts, one host and one network, or two networks. When one endpoint is a single computer, the VPN connection will extend all the way to that computer, where the data is encrypted and decrypted. If one end point is a network, the connection will end at a **Security Gateway**, which manages the VPN functions for the rest of the network. The data transmission within the network, between the security gateway and client computers, is not encrypted.

Data transfer between two computers over a **Public Wide Area Network (WAN)** uses public routers, switches, and other network components. This is, in general, not secure as messages can be read in clear text at every point between the end computers. An **IPSec VPN**, however, builds a secured **IP Security (IPSec)** tunnel through the public **WAN**. Messages sent through this tunnel cannot be read.

An **IPSec** tunnel consists of a two directional **Security Associations (SAs)**, one for each direction of communication.

An **IPSec SA** consists of three components:

- the **Security Parameter Index (SPI)**,
- the IP address of the receiver,
- a **Security Protocol Authentication Header (AH)** or **Encapsulated Security Payload (ESP)**.

With the help of the **SA**, the **IPSec VPN** tunnel has the following features:

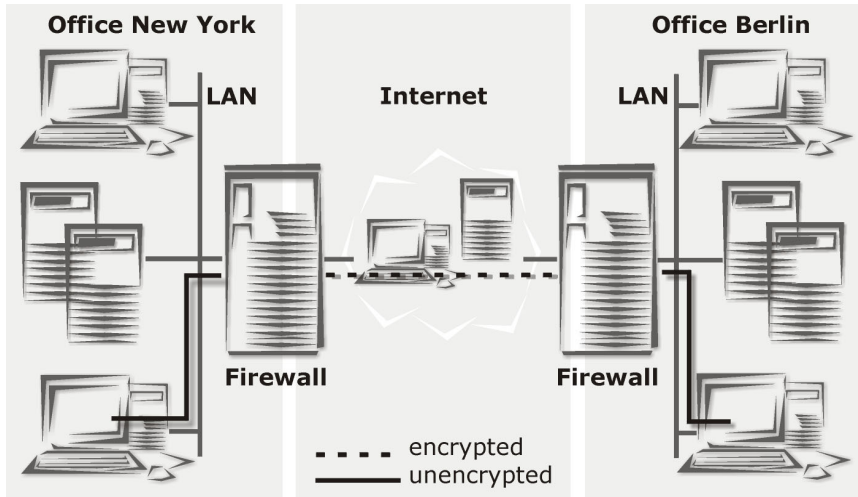
- Data confidentiality through encryption
- Data integrity through data authentication
- Sender authentication through PSK, RSA, or X.509 certificates

The security features can be combined as desired. Most administrators use at least the encryption and authentication components.

There are a few scenarios where VPNs can be used:

Using the Security System

1. Net-to-Net Connection

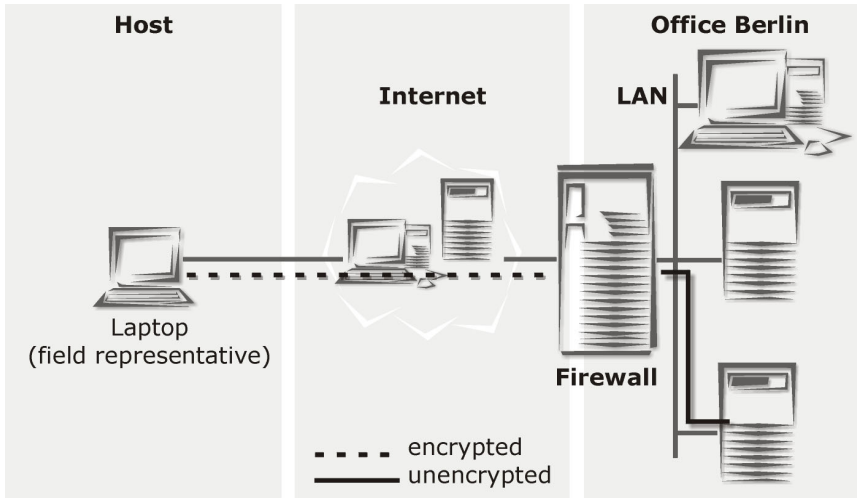


In this scenario, one network communicates with another.

Two remote offices can use a VPN tunnel to communicate with each other as though they were on a single network.

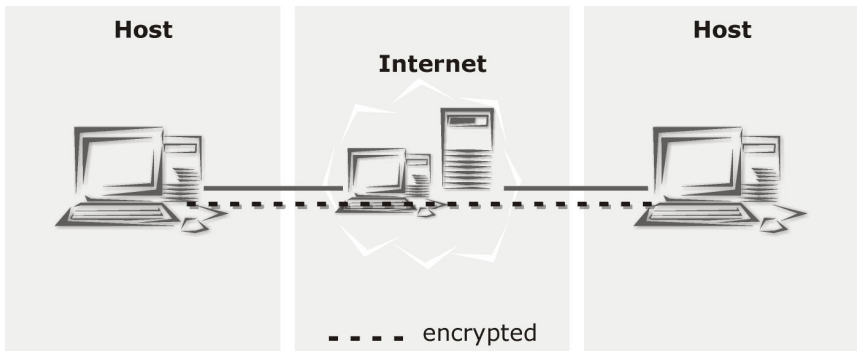
This kind of connection can also be used to allow trusted third companies (e.g., consultants and partner firms) access to internal resources.

2. Host-to-Net Connection



In this scenario a single computer communicates with a network. Telecommuters can use VPN to communicate with the main office securely.

3. Host-to-Host Connection



In this scenario one computer communicates with another computer. Two computers can use a VPN tunnel to communicate securely over

Using the Security System

an untrusted network.

A VPN server is a cost effective and secure solution for transferring sensitive data, and can replace existing expensive direct connections and private lines.

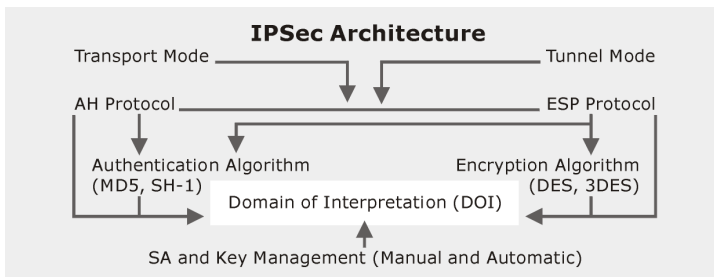
The IPSec Concept

IP Security (IPSec) is a suite of protocols designed for cryptographically secure communication at the IP layer (layer 3). (see also chapter 1, on page 9).

The IPSec standard defines two service modes and two protocols:

- **Transport Mode**
- **Tunnel Mode**
- **Authentication Header (AH)** Authentication protocol
- **Encapsulated Security Payload (ESP)** Encryption (and Authentication) protocol

IPSec also offers methods for manual and automatic management of **Security Associations (SAs)** as well as key distribution. These characteristics are consolidated in a **Domain of Interpretation (DOI)**.

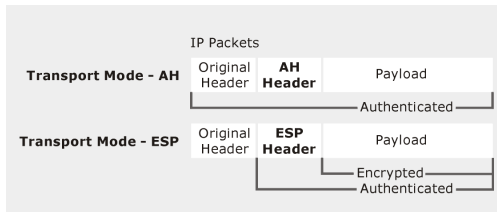


Note:

This security system uses the **Tunnel Mode** and the **Encapsulated Security Payload (ESP)** protocol.

IPSec Modes

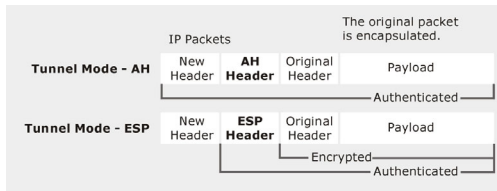
IPSec can work in either **Transport Mode** or **Tunnel Mode**. In principle, a host-to-host connection can use either mode. If, however, one of the endpoints is a security gateway, the Tunnel Mode must be used. The IPSec VPN connections on this security system always use the Tunnel Mode.



In **Transport Mode**, the original IP packet is not encapsulated in another packet. The original IP header is retained, and the rest of the packet is sent

either in clear text (**AH**) or encrypted (**ESP**). Either the complete packet can be authenticated with **AH**, or the payload can be encrypted and authenticated using **ESP**.

In both cases, the original header is sent over the WAN in clear text.



In **Tunnel Mode**, the complete packet – header and payload – is encapsulated in a new IP packet. An IP header is added to the IP-packet, with the destination

address set to the receiving tunnel endpoint. The IP addresses of the encapsulated packets remain unchanged. The original packet is then encrypted and/or authenticated in its entirety. The **AH** protocol allows the entire packet to be authenticated.

Using the Security System

IPSec-Protocols

IPSec uses two protocols to communicate securely on the IP level.

- **Authentication Header (AH)** – a protocol for the authentication of packet senders and for ensuring the integrity of packet data
- **Encapsulating Security Payload (ESP)** – a protocol for encrypting the entire packet and for the authentication of its contents.

Das **Authentication Header-Protocol (AH)** checks the authenticity and integrity of packet data. In addition, it checks that the sender and receiver IP addresses have not been changed in transmission. Packets are authenticated using a checksum created using a Hash-based Message Authentication Code (HMAC) in connection with a key. One of the following hashing algorithms will be used:

Message Digest Version 5 (MD5) This algorithm generates a 128-bit checksum from a message of any size. This checksum is like a fingerprint of the message, and will change if the message is altered. This hash value is sometimes also called a **digital signature** or a **message digest**.

The **Secure Hash (SHA-1)** algorithm generates a hash similar to that of **MD5**, though the SHA-1 hash is 160 bits long. **SHA-1** is more secure than **MD5**, due to its longer key.

Compared to **MD5**, an **SHA-1** hash is somewhat harder to compute, and requires more CPU time to generate. The computation speed depends, of course, on the processor speed and the number of **IPSec VPN** connections in use at the **Security Gateway**.

In addition to encryption, the **Encapsulated Security Payload Protocol (ESP)** offers the ability to authenticate senders and verify packet contents. If **ESP** is used in **Tunnel Mode**, the complete IP packet (header and payload) is encrypted. New, unencrypted IP and ESP headers are added to the encapsulating packet: The new IP header contains the address of the receiving gateway and the address

of the sending gateway. These IP addresses are those of the VPN tunnel.

For **ESP** with encryption normally the following algorithms are used:

- Triple Data Encryption Standard (3DES)
- Advanced Encryption Standard (AES)

Of these, AES offers the highest standard of security. The effective key lengths that can be used with AES are 128, 192 and 256 Bits. This security system supports a number of encryption algorithms.

Either the MD5 or SHA-1 algorithms can be used for authentication.

Key Management

The secure generation, management, and distribution of keys is crucial to the security of IPSec connections. IPSec supports both manual and automatic key distribution.

Manual key distribution requires that both sides of the connection be configured by hand. This means that for every **Security Association (SA)** (there are two per tunnel), a **Security Parameter Index (SPI)** must be selected, a key for encryption and authentication must be generated, and the keys must be installed on both sides of the tunnel. These keys should also be changed at regular intervals.

Clearly, manual distribution is labor-intensive. Because of the complexity of the process, manual intervention intensifies the risk that an unauthorized party gains access to the keys.

For these reasons, **Manual Key Distribution** is not often used.

The **Internet Key Exchange (IKE)** protocol provides **IPSec** with automatic key management capabilities. Keys are automatically generated and securely exchanged. **IKE** also allows the generation and management of multiple VPN tunnels and the use of dynamic IP addresses. The **IKE** protocol automatically manages the **Security Associations (SAs)** for a connection.

Using the Security System

This system supports three kinds of authentication for IKE:

- IKE with Preshared Keys (PSK)
- IKE with RSA Keys (RSA)
- IKE with X.509v3 Certificates (X.509)

Authentication with **Preshared Keys (PSK)** uses secret passwords as keys – these passwords must be distributed to the endpoints before the connection is built. When a new VPN tunnel is built, each side checks that the other knows the secret password. The security of such **PSKs** depends on how “good” the passwords used are: common words and phrases are subject to dictionary attacks. Permanent or long-term IPsec connections should use certificates or RSA keys instead.

Authentication via **RSA Keys** is much more sophisticated. In this scheme, each side of the connection generates a key pair consisting of a **Public Key** and a **Private Key**. The **private key** is necessary for the encryption and authentication during the **Key Exchange**. Both keys are mathematically independent from each other and are in a unique relation to each other: Data encrypted with one key can only be decrypted with the other. The **Private Key** cannot be deducted with maintainable work from the **Public Key**.

Both receivers of an IPsec VPN connection require in this authentication method their own **Public Key** and **Private Key**.

Similarly, the **X.509 Certificate** authentication scheme uses **public keys** and **private keys**. An X.509 certificate contains the **public key** together with information identifying the owner of the key. Such certificates are signed and issued by a trusted **Certificate Authority (CA)**. During the **Key Exchange** process, the certificates are exchanged and authenticated using a locally stored CA certificate.

Further information on **Certificate Authorities (CAs)** can be found in chapter 5.1.9 on page 94 and in chapter 5.7.6 on page 290.

5.7.1. Connections

The **Connections** menu allows you to configure local settings for new **IPSec VPN** tunnels and to manage existing connections.

Global IPSec Settings

The screenshot shows two overlapping windows from a security system interface. The top window, titled 'Global IPSec Settings', has a 'Status' section with a green indicator and a 'Disable' button, and an 'IKE Debugging' section with a red indicator and an 'Enable' button. The bottom window, titled 'New IPSec Connection', contains several configuration fields: 'Name' (text box with 'vpn'), 'Type' (dropdown menu with 'Standard'), 'IPSec Policy' (dropdown menu with 'Please select :'), 'Auto packet filter' (dropdown menu with 'On'), 'Strict Routing' (dropdown menu with 'On'), 'Endpoint Definition' section with 'Local Endpoint' and 'Remote Endpoint' (both dropdown menus with 'Please select :'), 'Subnet definition (optional)' section with 'Local Subnet' and 'Remote Subnet' (both dropdown menus with 'None :'), and 'Authentication of remote Station (s)' section with a 'Key' dropdown menu with 'Please select :'. An 'Add' button is located next to the 'Name' field.

This section allows you to enable or disable the **IPSec VPN** system by clicking the **Enable/Disable** button next to **Status**.

IKE Debugging: This function allows you to check the IPSec connection. Detailed information is logged to the IPSec logs. These protocols can be displayed in real time in the **Local Log/IPSec VPN** menu or downloaded to your local computer.

Further information on the **Local Logs** menu can be found in chapter 5.9 on page 307.

Important Note:

The **IKE Debugging** function requires a large amount of system resources, and can slow the IPSec VPN connection building process down considerably. This system should only be enabled when IKE is actively being debugged.

Using the Security System

IPSec Connections

In the **IPSec Connections** table, all current VPN connections are listed.

IPSec System Information



VPN Status: In the **VPN Status** window, status information is shown for ac-

tive encryption algorithms, all active IPSec connections, and detailed information about every **Security Association (SA)**.

VPN Routes: The **VPN Routes** window shows all active IPSec SA connections. If no entries exist here, no IPSec connections are active.

Routing entries follow the following form:

```
A B                      -> C                      => D
3 192.168.105.0/24 -> 192.168.104.0/24 => %hold
8 192.168.105.0/24 -> 192.168.110.0/24 => %trap
0 192.168.105.0/24 -> 192.168.130.0/24 =>
                               tun0x133a@233.23.43.1
```

Column **A**: The number of packets in this VPN connection.

Column **B**: The local subnet or host.

Column **C**: The remote subnet or host.

Column **D**: The status of the connection.

%trap: The connection is idle and is waiting for a packet. The status initiates the end of the VPN connection.

%hold: The connection is being negotiated. All packets will wait until the VPN tunnel is established (UP).

tun0x133a@233.23.43.1: Messages like these show that the tunnel is up.

A VPN tunnel with ID 0x133a has been established, and the IP address of the **Remote Endpoint** is 233.23.43.1..

Example:

```
A B                -> C                => D
23 192.168.105.0/24 -> 192.168.104.0/24 =>
                        tun0x1234@123.4.5.6
```

This message shows that 23 data packets have been sent from network 192.168.105.0/24 to network 192.168.104.0/24. The tunnel's ID number is 0x1234, and the remote endpoint is has IP address 123.4.5.6..

Configuring an IPSec Connection:

1. Under the **IPSec VPN** tab, open the **Connections** menu.
2. Enable the option by clicking the **Enable** in the **Global IPSec Settings** window.

The **New IPSec Connection** window will open.

3. In the **Name** field, enter a descriptive name for the new IPSec VPN connection:

Name: Enter a descriptive name for this IPSec-VPN tunnel. Allowed characters are: Only alphanumeric and underscore characters are allowed.

Type: Choose the type of connection to use.

Use **Standard** for **Net-to-Net** connections.

The **Road Warrior**, **Road Warrior CA** and **MS Windows L2TP IPSec** connection types are useful with **HOST-to-NET** connections, e.g. for sales representatives. The telecommuter will then be able to build an IPSec connection to the firm's internal network. A road warrior connection can only be used through a **default gateway**.

Note:

Multiple remote key objects can be added to a single road warrior connection. This can serve to reduce configuration hassles. It must be respected, however, that all road warriors use the same type of authentication (PSK, RSA or X.509) – a mixed operation can result in malfunctions.

Further configuration parameters can be set for the chosen connection type.

4. Make the following basic settings for the IPSec-VPN connection.

IPSec Policy: The policy controls the parameters for the VPN connection. This includes the settings for **Key Exchange, IKE,** and the **IPSec** connection.

The drop-down menu contains a number of pre-defined policies. You can define custom ones in the **IPSec VPN/Policies** menu.

Note:

A standard policy is used for the **MS Windows L2TP IPSec** type of connection.

The configuration of **IPSec Policies** is detailed in chapter 5.7.2 on page 277.

Auto Packet Filter: Once the IPSec-VPN connection is successfully established, the packet filter rules for the data traffic will automatically be added. After the completion of the connection, the packet filter rules will be removed.

The **Auto Packet Filter** function is available for the **Standard** and **road warrior** connection types.



Security Note:

If you want greater control over the packet filter rules, or wish to manage them in a more centralized way, disable the **Auto Packet Filter** function and enter the rules manually in the **Packet Filter/Rules** menu.

Strict Routing: When this function is enabled (**On**), VPN Routing is not only done with the destination address, but in harmony with the source and destination address.

If *Strict Routing* is enabled, it is possible to simultaneously set encrypted and decrypted connections from different source addresses to one network.

If the **Strict Routing** function is disabled (**Off**), further networks and hosts can be connected to the IPSec-VPN tunnel through the setting of **Source NAT** rules.

The **Strict Routing** function can only be disabled or enabled in the **Standard** type of connection. For all other types of connections the function is always enabled!

5. In the **Endpoint Definition** window, select the endpoint of the IPSec tunnel.

Local Endpoint: Use the drop-down menu to select the local endpoint. Always choose the network interface on the same side of the firewall as the remote endpoint.

Remote Endpoint: Choose the IP address of the remote endpoint here.

With the *Road Warrior* or *MS Windows L2TP IPSec* types of connection, the remote endpoint has always a dynamic IP address.

6. The **Subnet definition (optional)** window allows you to set an optional subnet for both endpoints.

Local Subnet: Choose the local subnet here.

Remote Subnet: Choose the remote subnet here.

Using the Security System

With a **road warrior** connection, only the local subnet can be configured. This is no more possible if you additionally enable the **L2TP Encapsulation** function in step 7.

Note:

With the **MS Windows L2TP IPsec** connection this window will not be displayed. The IPsec-VPN access will be managed through the **Packet Filter**.

7. Select the associated **key** in the **Authentication of Remote Station(s)** window.

IPsec remote keys are defined in the **IPsec VPN/Remote Key** menu. The settings in this window depend on the type of connection.

7.1 Standard

Key: Use the drop-down menu to select a **Remote Key**.

7.2 Road Warrior

L2TP Encapsulation: This drop-down menu allows you to additionally enable **L2TP over IPsec (On)**.

Keys: Select the **Remote Keys** for the road warrior connection from the selection window.

7.3 Road Warrior CA

L2TP Encapsulation: This drop-down menu allows you to additionally enable **L2TP over IPsec (On)**.

Use CA: With the *road warrior CA* connection type, the authentication is based on the **Distinguished Name (DN)** of the remote receiver (**Remote Endpoint**). You thus need a **Certificate Authority (CA)** from this endpoint. Only the VPN Identifier **X.509 DN** can be used.

From the drop-down menu, select **X.509 DN Certificate Authority (CA)**.

Client DN Mask: In order to use a **Distinguished Name** as an ID, you will need the following information from the X.509 index: Country (C), State (ST), Local (L), Organization (O), Unit (OU), Common Name (CN) und E-Mail Address (E).

The data in this entry field must be in the same order as in the certificate.

7.3 MS Windows L2TP IPsec

L2TP Encapsulation: With this type of connection, **L2TP over IPsec** is automatically enabled (**On**).

IPsec Shared Secret: With the *MS Windows L2TP IPsec* connection type, the authentication is based on Preshared Keys.

Enter the password into this entry field.

8. Save these settings by clicking **Add**.

The newly configured IPsec profile will appear, deactivated, at the bottom of the table (status light is red). Clicking on the status light enables the IPsec connection.

After you configure a new VPN tunnel, you will need to establish the related packet filter rules to allow the two computers to communicate. Configuring packet filter rules is described in chapter 5.4 on page 179.

Using the Security System

Example:

In order to set-up a Net-to-Net VPN connection (between network 1 and network 2), you will need to define the following rules:

1. Under the **Packet Filter** tab, open the **Rules** menu.
2. In the **Add Rules** window, add the following rule for network 1:
Source: Network1
Service: Any
Destination: Network 2
Action: Allow
3. Confirm the entries by clicking on **Add Definition**.
4. In the **Add Rules** window, add the following rule for network 2:
Source: Network 2
Service: Any
Destination: Network1
Action: Allow
5. Confirm the entries by clicking on **Add Definition**.

These rules will allow complete access between the two networks.

5.7.2. Policies

IPSec Policies					New
Name	Protocol	Encryption	Features	Actions	
3DES	ESP	3DES	[none]	edit	delete
3DES_COMP	ESP	3DES	deflate	edit	delete
3DES_PFS	ESP	3DES	PFS	edit	delete
3DES_PFS_COMP	ESP	3DES	PFS,deflate	edit	delete
ACM_Default	ESP	AES128	deflate	edit	delete
AES	ESP	AES128	[none]	edit	delete
AES_COMP	ESP	AES128	deflate	edit	delete
AES_PFS	ESP	AES128	PFS	edit	delete
AES_PFS_COMP	ESP	AES128	PFS,deflate	edit	delete
BLOWFISH	ESP	3DES	[none]	edit	delete
MS_DEFAULT	ESP	3DES	[none]	edit	delete
NULL	ESP	NULL	[none]	edit	delete

In the **Policies** menu, you can customize parameters for IPSec connections and collect them into a policy. Policies are used to define

New IPSec Policy

Name: Add

Key Exchange: **IKE**

ISAKMP (IKE) Settings

IKE Mode: Main Mode

Encryption Algorithm: 3DES 168bit

Authentication Algorithm: MD5 128bit

IKE DH Group: DH Group 5 (MODP1536)

SA Lifetime (secs): 7800

IPSec Settings

IPSec Mode: Tunnel

IPSec Protocol: ESP

Encryption Algorithm: 3DES-CBC 168bit

Enforce Algorithms: Off

Authentication Algorithm: MD5 128bit

SA Lifetime (secs): 3600

PFS: PFS Group 5 (MODP1536)

Compression: Off

IPSec connections, and contain the configuration of the selected **key exchange** method, **IKE**, and the **IPSec** connection.

The chosen **key exchange** method defines how the keys for the connection are to be managed.

The two exchange methods are:

- Manual Key Exchange
- Internet Key Exchange (IKE)

Because of the complexity of manual exchange, this system only supports the IKE key exchange method. Manual exchange is not allowed.

Using the Security System

Configuring an IPSec Policy:

1. Under the **IPSec VPN** tab, open the **Policies** menu.
2. Click **New** to open the **New IPSec Policy** menu.
3. In the **Name** field, enter a name for the new policy:

Name: Enter a name describing the policy. It may be useful to include the encryption algorithm in the name. The name can also be defined as the last step in creating the policy.

Key Exchange: Only **IKE** is supported.

4. In the **ISAKMP (IKE) Settings** window, configure the settings for IKE:

IKE Mode: The IKE mode is used to support key exchange. At the moment, only the **Main Mode** is supported.

Encryption Algorithm: The encryption algorithm is the algorithm used to encrypt IKE connections. The IPSec VPN function of this security system supports **1DES 56bit**, **3DES 168bit**, **AES (Rijndael) 128bit**, **AES Rijndael 192bit**, **AES Rijndael 256bit**, **Blowfish**, **Serpent 128bit** and **Twofish**.

Authentication Algorithm: The hashing algorithm ensures the integrity of the IKE messages. The **MD5 128bit**, **SHA1 160bit**, **SHA2 256bit** and **SHA2 512bit** algorithms are supported. The algorithm used is determined by the remote endpoint of the IPSec connection.

Important Note:

The **SHA2 256bit** and **SHA2 512bit** algorithms require a great deal of system resources.

IKE DH Group: The IKE group (Diffie-Hellmann group) describes the kind of asymmetric encryption used during key exchange. The IPSec VPN system on this security system supports the **Group 1 (MODP768)**, **Group 2 (MODP 1024)**, **Group 5 (MODP 1536)**, **Group X (MODP 2048)**, **Group X**

(MODP 3072) and **Group X (MODP 4096)** protocols. The group used is determined by the remote endpoint.

SA lifetime (secs): This option allows you to set the lifetime of IKE sessions in seconds. This is set by default to 7800 seconds (2h, 10 min).

In general, times between 60 and 28800 seconds (1 min to 8 hours) are allowed.

5. In the **IPSec Settings** window, configure the settings for the IPSec connection:

IPSec Mode: This system only supports **tunnel mode**.

IPSec Protocol: This system only supports **ESP**.

Encryption Algorithm: Choose the encryption algorithm to use here. The IPSec VPN function of this security system supports **1DES 56bit, 3DES 168bit, AES (Rijndael) 128bit, AES Rijndael 192bit, AES Rijndael 256bit, Blowfish, Serpent 128bit** and **Twofish**. If you wish to create IPSec connections without encryption, choose **null** here.

Enforce Algorithm: If an IPSec Gateway makes a proposition with respect to an encryption algorithm and to the strength, it might happen, that the gateway of the receiver accepts this proposition, even though the IPSec Policy does not correspond to it. In order to avoid this, **Enforce Algorithm** must be enabled.

Example:

The IPSec Policy requires AES-256 as encryption. Whereas a road warrior with **SSH Sentinel** wants to connect with AES-128. Without **Enforce Algorithm** the connection will be admitted, which constitutes a security risk.

Authentication Algorithm: The **MD5 128bit, SHA1 160bit, SHA2 256bit** and **SHA2 512bit** algorithms are supported. The algorithm used is determined by the remote endpoint of the IPSec connection.

Using the Security System

Important Note:

The **SHA2 256bit** and **SHA2 512bit** algorithms require a great deal of system resources.

SA Lifetime (secs): This option allows you to set the lifetime of the IPSec connection. This is set by default to 3600 seconds (1h). In general, times between 60 and 28800 seconds (1 min to 8 hours) are allowed.

PFS: The IPSec key used for VPN connections is generated from random numbers. When **Perfect Forward Secrecy (PFS)** is enabled, the system will ensure that the numbers used have not already been used for another key, such as for an IKE key. If an attacker discovers or cracks an old key, he or she will have no way of guessing future keys.

The IPSec VPN system on this security system supports the **Group 1 (MODP768)**, **Group 2 (MODP 1024)**, **Group 5 (MODP 1536)**, **Group X (MODP 2048)**, **Group X (MODP 3072)** and **Group X (MODP 4096)** protocols. If you do not wish to use **PFS**, select **No PFS**.

By default, this is set to **Group 5 (MODP 1536)**.

Important Note:

PFS requires a fair amount of processing power to complete the **Diffie-Hellmann** key exchange. **PFS** is also often not 100% compatible between manufacturers. In case of problems with the firewall's performance or with building connections to remote systems, you should disable this option.

Compression: This algorithm compresses IP-packets before they are encrypted, resulting in faster data speeds.

This system supports the Deflate algorithm.

6. If you have not yet named this policy, scroll back to the **Name** field and enter one now.

Using the Security System

7. Create the new policy by clicking **Add**.

The new **policy** will appear in the **IPSec Policies** table.

Using the Security System

5.7.3. Local Keys

The image shows two overlapping configuration windows from a security system. The top window is titled 'Local IPsec X.509 Key' and contains a 'Local Certificate:' dropdown menu, a 'Passphrase:' text field, and a 'Save' button. The bottom window is titled 'Local IPsec RSA Key' and contains a 'VPN Identifier:' dropdown menu with 'IPv4 Address' selected, a note stating 'Local tunnel IP address will be selected automatically', a 'Save' button, a paragraph of instructions: 'Please select a key size and click Save to generate the local RSA key. A key size of at least 2048 bits is recommended.', an 'RSA Key Length:' dropdown menu, and another 'Save' button.

The **Local Keys** menu allows an administrator to manage local **X.509** certificates, to define the local IPsec identifier, and to generate a local RSA key pair.

Local IPsec X.509 Key

In this window, you can define keys for **X.509** certificates provided you have already generated these certificates in the **IPsec VPN/CA Management** menu.

Chapter 5.7.6 on page 290 describes the process of generating X.509 certificates.

If you wish to use **X.509** authentication, use the **Local certificate** drop-down menu to select the certificate. This menu only contains those certificates for which the associated **private key** is available.

In the **Passphrase** field, enter the password used to secure the **private key**.

The **active key** will appear with its name in the **Local IPsec X.509 Key** window. If you choose a new local key, the old key will automatically be replaced.

The firewall will use the ID and public/private keypair of the current local Local X.509 key to sign, authenticate, and encrypt X.509 IPsec key exchanges.

RSA Authentication

RSA authentication requires a **Local IPSec Identifier** and a **Local RSA Key**.

Note:

Depending on the selected key length and the processor of the security solution, the generation of **RSA keys** can take several minutes.

1. In the **Local IPSec RSA Key** window, define a unique **VPN Identifier**.

IPv4 Address: For static IP addresses.

Hostname: For VPN security gateways with dynamic addresses.

E-Mail Address: For mobile (road warrior) connections.

Save the settings by clicking **Save**

2. Generate a new RSA Key in the **Local RSA Key** window, by selecting the key length from the **RSA Key length** drop-down menu.
3. When you click **Save**, the system will begin generating a new RSA key pair.

After generation, the active **Local RSA Key** and its name will be displayed. When a new key is generated, the old key will be replaced.

Using the Security System

PSK Authentication

For authentication through **Preshared Keys (PSK)**, no additional configuration of local keys is required.

During the key exchange using **IKE Main Mode**, only **IPv4 Addresses** are supported as IPSec identifiers. The IPSec identifier in the **IKE Main Mode** is automatically encrypted with the **PSK**, and so **PSK** cannot be used for authentication. The IP addresses of IKE connections are automatically used as **IPSec identifiers**.

The **PSK Key** is entered in the **IPSec Policies/Remote Keys** menu. It will automatically be used as the **Local PSK Key** as well.

5.7.4. Remote Keys

The screenshot shows a 'New Remote IPSec Key' dialog box with the following fields:

- Name:
- Virtual IP (optional):
- Key Type:

Below the dialog box are two tables:

Remote Keys				
Name	Type	ID	Virtual IP (optional)	User config download
:: No remote keys defined ::				

CA Management Remote Keys				
Name	VPN ID	Virtual IP (optional)	User config download	Actions
:: No host certificates defined in CA Management ::				

IPSec remote key objects can be defined in the **Remote Keys** menu. An IPSec-Remote-Key-Object represents an IPSec receiver. This receiver can either be a security gate-

way, a host or also a road warrior with dynamic IP-address.

An IPSec remote key object is defined by three parameters:

- The IKE authentication method (PSK/RSA/X.509)
- The IPSec ID of the remote endpoint (IP/Hostname/E-Mail Address/Certificate)
- The authentication data (Shared secret for PSK, public key for RSA, X.509 certificate)

Every IPSec remote endpoint must have an associated IPSec remote key object defined.

Defining IPSec Remote Keys:

1. Under the **IPSec VPN** tab, open the **Remote Keys** menu.

The **New Remote IPSec Key** will immediately be displayed.

2. In the **Name** field, enter a name for the new **Remote Key**.

Virtual IP Key If you wish to use the IPSec Remote Key for a standard connection, continue with step 3.

Virtual IP Key (optional): This function allows you to assign a virtual IP address to the road warrior. This is the only way to manually set IP addresses for such connections. If you enter an IP address here, it must also be configured on the road warrior system.

Using the Security System

Attention:

With a road warrior IPSec tunnel, the **Virtual IP Key** function must be enabled if you wish to use the **NAT Traversal** function and the L2TP Encapsulation function is disabled.

The IP address entered here should not be used anywhere else, and cannot be a part of a directly connected network.

3. Use the **Key type** drop-down menu to select the IKE authentication method. Further options are available depending on the chosen **Key type**.

PSK: The firewall only supports using **IPv4 Addresses** as **VPN Identifiers** during the key exchange phase of **IKE Main Mode**.

Enter the shared password in the **Preshared Key** field.

If you wish to configure many road warrior connections, you only need one PSK for all connections.

Security Note:



Use a secure password! Your name spelled backwards is, for example, not a secure password – while something like xft35\$4 would be. Make certain that this password does not fall into the wrong hands. With this password, an attacker can build a VPN connection to the internal network. We recommend changing this password at regular intervals.

RSA: The key pair consists of a **private key** and a **public key**. In order for the endpoints to communicate, they must exchange their **public keys**. **Public keys** can be exchanged via e-mail.

In the **VPN Identifier** drop-down menu, choose the VPN ID type of the endpoint. If you select **E-Mail Address, Full qualified domain name** or **IP Address**, you must enter the address or name in the entry field below.

X509: Use the **VPN Identifier** drop-down menu to select the kind of VPN ID to use. If you select **E-Mail Address, Full**

Using the Security System

qualified domain name or **IP Address**, you must enter the address or name in the entry field below.

In order to use a **Distinguished Name** as an ID, you will need the following information from the X.509 index: Country (C), State (ST), Local (L), Organization (O), Unit (UO), Common Name (CN) und E-Mail Address (E-Mai).

4. To save the new IPSec remote key object, click **Add**.

The new remote key object will appear in the **Remote Keys** table.

CA Management Remote Keys are shown in a separate table.

Using the Security System

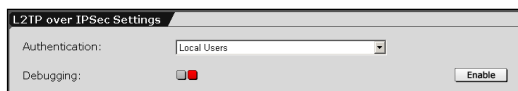
5.7.5. L2TP over IPSec

L2TP over IPSec is a combination of the *Layer 2 Tunneling Protocol* and of the *IPSec* standard protocol. **L2TP over IPSec** allows you, while providing the same functions as PPTP, to give individual hosts access to your network through an encrypted IPSec tunnel. On Microsoft Windows systems, **L2TP over IPSec** is easy to set-up, and requires no special client software.

For the MS-Windows systems 98, ME and NT Workstation 4.0, **Microsoft L2TP/IPSec VPN Client** must first be installed. This client is available from Microsoft at:

<http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/l2tpclient.asp>

L2TP over IPSec Settings



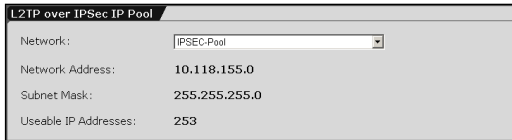
Authentication: Use this drop-down menu to configure the authentication

method. If you have defined a RADIUS server in the **System/User Authentication** menu, you can use it here as well.

The configuration of the Microsoft IAS RADIUS server and the configuration of RADIUS within WebAdmin is described in chapter 5.1.7 on page 71.

Debugging: This function allows you to check the L2TP-over-IPSec connection. Detailed information is logged to the IPSec logs. These protocols can be displayed in real time in the **Local Log/Browse** menu or downloaded to your local computer. Further information about the **Local Logs** menu can be found in chapter 5.9 on page 307.

L2TP over IPSec IP Pool



The screenshot shows a configuration window titled "L2TP over IPSec IP Pool". It contains the following fields:

Network:	IPSec-Pool
Network Address:	10.118.155.0
Subnet Mask:	255.255.255.0
Useable IP Addresses:	253

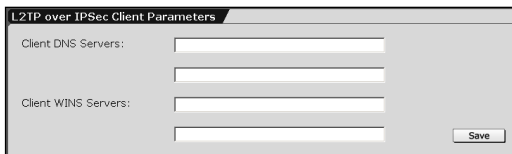
This menu is used to define which IP addresses PPTP hosts should be assigned to. By default, a network from the private

IP range 10.x.x.x will be selected when the L2TP-over-IPSec function is enabled for the first time. This network is referred to as **IPSec Pool** and can also be used for all other functions of the Security system, using network definitions. If you wish to use a different network, simply change the definition of the *IPSec-Pool*, or assign another defined network as *IPSec-Pool* here.

Note:

If you use private IP addresses for your **IPSec Pool**, such as the pre-defined network and you wish IPSec hosts to be allowed to access the Internet, appropriate **Masquerading** or **NAT** rules must be in place for the *IPSec Pool*.

L2TP over IPSec Client Parameters



The screenshot shows a configuration window titled "L2TP over IPSec Client Parameters". It contains the following fields:

Client DNS Servers:	<input type="text"/>
	<input type="text"/>
Client WINS Servers:	<input type="text"/>
	<input type="text"/>

There is a "Save" button at the bottom right of the window.

This window allows you to define DNS and WINS servers which should be assigned to hosts when the connection is established.

Using the Security System

5.7.6. CA Management

A **Certificate Authority (CA)** certifies the authenticity of public keys. This ensures that the certificate used in a VPN connection really belongs to the endpoint, and not to an attacker. The **CA Management** menu allows you to create and manage your own **X.509 Certificate Authority (CA)**. The authority will verify the validity of X.509 certificates exchanged during IPSec VPN connections. The relevant information is stored in the X.509 certificates.

But you can also use certificates, signed by commercial providers, such as VeriSign.

Note:

Every certificate has unique **CA** with respect to its identifying information (Name, Firm, Location, etc.). If the first certificate is lost, a second cannot be generated to replace it.

The **CA Management** menu allows you to manage three distinct kinds of certificates, which are used for different purposes. The three certificates differentiate themselves according to use, and, importantly, whether or not the **Private Key** is stored:

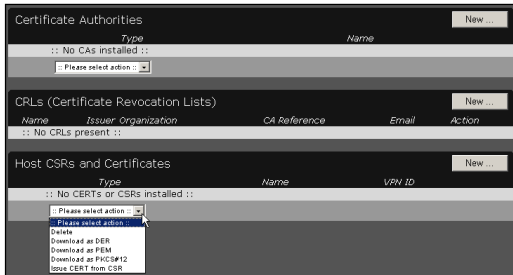
CA (Certificate Authority) Certificate: If a **CA** is saved without **private key**, it can be used for the authentication of the host and user certificate of incoming IPSec connections: this type of CA is called a **Verification CA**.

If a **CA** saves its **private key**, it can be used to sign certificate queries, in order to produce a valid certificate. This **CA** is called a **Signing CA**.

The system can contain a number of **Verification CAs**, but only one **Signing CA**.

Host CSR (Certificate Signing Request): This is a request to have a certain certificate signed. When it is given to a **Signing CA** - and the CA verifies the identity of the owner - the CA sends back a fully-formed and signed **Host Certificate**.

Host Certificate: This certificate contains the **public key** of the host as well as identifying information about the host (such as IP address or owner). The certificate is also signed by a **CA**, verifying that the **key** does indeed belong to the entity named in the identification information. These valid certificates are used to authenticate remote IPSec hosts/user endpoints.



The drop-down menu at the bottom of the table allows you to download certificates in various formats, or to delete certificates from the system:

PEM: A format encoding the certificate in ASCII code. The certificate, request, and private key are stored in separate files.

DER: A binary format for encoding certificates. The certificate, request, and private key are stored in separate files.

PKCS#12: A “container file”. One file can contain the certificate, private key, and verification CA.

Delete: Delete the specified certificate.

Issue CERT from CSR: This function signs a **CSR**, generating a full host certificate.

Using the Security System

Generating a Client/Host Certificate:

Step 1: Create a **Signing CA**.

1. Under the **IPSec VPN** tab, open the **CA Management** menu.
2. In the **Certificate Authorities** table, click the **New** button.
The **Add Certificate Authority** window will open.
3. Select the **Generate** option.
4. In the **Name** field, enter a descriptive **Name** for the certificate authority.
Allowed characters are: Only alphanumeric and underscore characters are allowed.
5. Enter a password with at least four characters in the **Passphrase** field.
6. Use the **Key Size** drop-down menu to select the desired key length.
7. Use the drop-down menus and entry fields from **Country** to **E-Mail Address** to enter identifying on the **CA**.
8. To save the entries, click the on the **Start** button.

The **Signing CA** will be loaded into the **Certificate Authorities** menu. This CA will answer **CSR** requests by generating new host certificates.

Step 2: Generate a **Certificate Request**.

1. In the **Host CSR or Certificate** table, click the **New** button.
The **Host CSR or Certificate** window will open.
2. Select the **Generate CSR** option.

In the **VPN ID** drop-down menu, select the type of VPN ID to use. If you select **E-Mail Address**, **Hostname** or **IPv4 Address**, you must enter the relevant information in the field at

right.

The field should be empty if you select the **X509 DN** option.

3. In the **Name** field, enter a descriptive name for this certificate request.

Allowed characters are: Only alphanumeric and underscore characters are allowed.

4. Enter a password with at least four characters in the **Passphrase** field.
5. Use the **Key Size** drop-down menu to select the desired key length.
6. Use the drop-down menus and entry fields from **Country** to **E-Mail Address** to enter identifying information about the **certificate holder**.

Common Name: If the CSR is for a road warrior connection, enter the name of the user here. If the CSR is for a host, enter the hostname.

7. To save the entries, click the on the **Start** button.

The Certificate Request **CSR + KEY** will appear in the **Host CSRs and Certificates** table. The table will also show the type, name, and VPN IP of the CSR. The request can now be signed by the **Signing CA** created in the first step.

Step 3: Generate the Certificate.

1. In the **Host CSRs and Certificates** table, select the **CSR + KEY** certificate request.
2. Use the drop-down menu at the bottom of the table to select the **Issue CERT from CSR** function.

An entry field labeled **Signing CA Passphrase** will appear. Enter the password of the **Signing CA** here.

3. Click **Start**.

Using the Security System

From the **CSR + KEY**, the CA will generate the **CERT + KEY** certificate: the certificate will replace the CSR in the table.

Step 4: Download the Certificate.

1. In the **Host CSRs and Certificates**, select the new certificate.
2. Use the drop-down menu at the bottom of the table to select a download format.

DER: In the **Passphrase** field, you must enter the password of the **Private Key**.

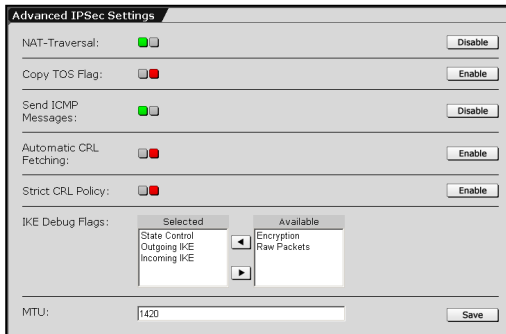
PEM: No password is necessary.

PKCS#12: Enter the password of the **Private Key** in the **Passphrase** field. In the **Export Pass** field, enter a different password. This password will be required to install the certificate on the client computer.

3. Click **Start**.

You must now install the certificate on the remote computer. The installation process depends on the IPSec software on that computer.

5.7.7. Advanced



This menu allows you, to make additional settings for the **IPSec VPN** option. This should, however, only be done by experienced users.

NAT Traversal: When enabled, **NAT Traversal** allows hosts to establish an

IPSec tunnel through NAT devices. This module attempts to detect if NAT firewalls are being used between the server and client: if so, the system will use UDP packets to communicate with the remote host. Please note that both IPSec nodes must support NAT traversal, and that road warrior nodes must be configured with a virtual IP address. In addition, IPSec passthrough must be turned off on the NAT device(s), as this can break NAT traversal.

Important Note:

You cannot use local IP addresses for the **Virtual IP** address, because the security system does not answer ARP requests for these.

Copy TOS Flag: Type-of-Service-Bits (TOS) are several four Bit-flags in the IP-header. The Bits are referred to as *Type-of-Service-Bits*, as they allow the transferring application, to tell the network which type of service quality is necessary. The available service quality classes are: minimum delay, maximum throughput, maximum reliability and minimum cost.

This function copies the content of the **Type-of-Service** field in the encrypted data packet, so that the IPSec data traffic can be routed according to its priority.

Enable the **Copy TOS Flag** function by clicking on the **Enable** button.

Using the Security System

Send ICMP Messages: If a data packet overwrites the configured **MTU** value, the system will send an ICMP message to the source address: Destination unreachable/fragmentation needed.

This allows for using Path MTU Discovery.

Automatic CRL Fetching: There might be situations, in which the provider of a certificate attempts to revoke the confirmation awarded with still valid certificates, for example if it has become known that the receiver of the certificate fraudulently obtained it by using wrong data (name, etc.) or because an attacker has got hold of the private key, which is part of the certified public key. For this purpose, so-called *Certificate Revocation Lists* or **CRLs** are used. They normally contain the serial numbers of those certificates of a certifying instance, that have been held invalid and that are still valid according to their respective periods of validity.

After the expiration of this periods the certificate will no longer be valid and must therefore not be maintained in the block list.

The **Automatic CRL Fetching** function automatically requests the *CRL* through the URL defined in the partner certificate via HTTP, Anonymous FTP or LDAP Version 3. On request, the *CRL* can be downloaded, saved and updated, once the validity period has expired. Enable the function by clicking on the **Enable** button (status light is green).

Please, check if the packet filter rules in the **Packet Filter/Rules** menu are configured such that the **CRL Distribution Server** can be accessed.

Strict CRL Policy: Any partner certificate without a corresponding *CRL* will be rejected.

Enable the function by clicking on the **Enable** button (status light is green).

Send ICMP Messages: If a data packet exceeds a set **MTU** value, the system will send the following ICMP message to the source address: Destination unreachable/fragmentation needed.

This allows for the use of Path MTU Discovery.

IKE debug Flags: This selection field allows you to configure the scope of IKE-debugging logs. The IKE Debugging function must be enabled in the **IPSec VPN/Connections** menu.

The following flags can be logged:

- State Control: control messages on the IKE status
- Encryption: Encryption and decryption operations
- Outgoing IKE: Content of outgoing IKE messages
- Incoming IKE: Content of incoming IKE messages
- Raw Packets: message in unprocessed bytes

MTU: Enter a the MTU value in this entry field.

By default the MTU value is already defined: 1420 Byte.

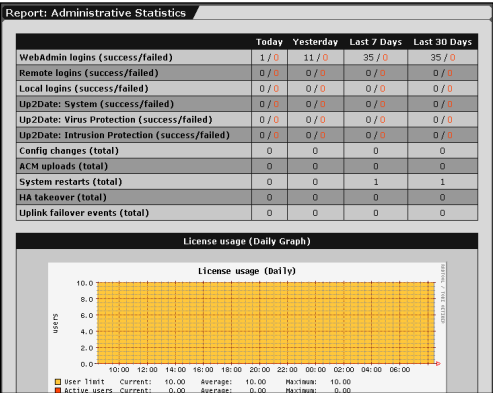
Using the Security System

5.8. System Management (Reporting)

The **Reporting** function provides current information about the system, the state of various subsystems, and real-time information about various reporting functions. The displayed values are updated every five minutes.

The diagrams shown on the first page of the **Reporting** menus show an overview of the current day's activity. By clicking the **Show all ...** button you can open a page containing graphics built from weekly, monthly, and yearly statistics.

5.8.1. Administration



The **Administration** menu contains an overview of the administrative events of the last 30 days.

The following events will be displayed:

- WebAdmin Logins
- Remote Logins
- Local Logins
- System Up2Dates
- Virus Pattern Up2Dates
- Intrusion Protection Pattern Up2Dates

- Config Changes
- Astaro Configuration Manager Uploads
- System Restarts
- High Availability Takeover

5.8.2. Virus

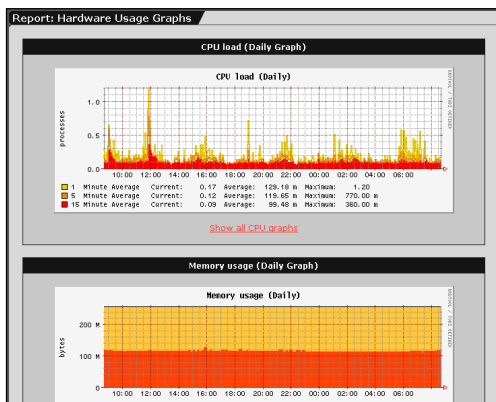
Report: Virus Protection Statistics				
	Today	Yesterday	Last 7 Days	Last 30 Days
SMTP viruses	0	0	0	0
POP3 viruses	0	0	0	0
HTTP viruses	0	0	0	0

The **Virus** menu contains an overview of the filtered viruses of the last 7 days.

The following viruses will be displayed:

- SMTP Viruses
- POP3 Viruses
- SMTP Viruses

5.8.3. Hardware



This menu shows the current values relating to your system hardware. The system collects statistics about CPU utilization, RAM utilization, and swap utilization.

The security system collects graphics and statistics every five minutes and updates them. The information can also be updated manually

by clicking on the **Reload** button. Don't use the **Refresh** button of the browser, because this will log you out of the **WebAdmin** configuration tool!

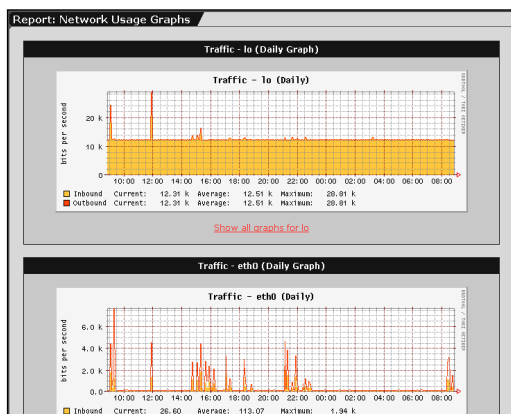
Using the Security System

CPU Load (Daily Graph): This diagram shows the current utilization of the CPU.

Memory Usage (Daily Graph): The current RAM utilization statistics are shown here. When more functions and subsystems are enabled on the firewall, more RAM will be required to support them.

SWAP Usage (Daily Graph): This diagram shows the current amount of swap space being used. Swap space is used to supplement **RAM**: if your system is running out of available RAM, you will see a sharp increase in swap usage.

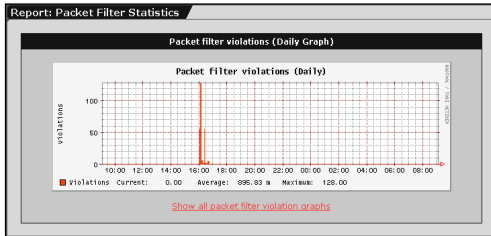
5.8.4. Network



This menu shows current statistics relating to network traffic. These diagrams will not be useful unless the network cards have been correctly configured in the **Network/Interfaces** menu.

The configuration process for network cards is described in chapter 5.3.2 on page 119.

5.8.5. Packet Filter



Packet filter violations in diagrams will be displayed in a graphic in this menu. The rule violations will also be logged to the **Packet Filter Logs**. The log files are saved to the **Local Logs/Browse** menu.

5.8.6. Content Filter

The processed data and actions of the **Content Filter**, relating to the HTTP, SMTP and POP3 proxies will be displayed in the form of tables and diagrams in this menu. The **Spam Protection** option and the **Spam Score** are described in chapter 5.6.6.2 on page 248.

Information on the SMTP and POP3 proxies:

- Sum of the treated messages
- The average size of messages in kilobytes
- The average height of *Spam Score*

Information on the HTTP proxy:

- Sum of requested HTTP-sites
- Sum of the HTTP-sites, blocked by *Spam Protection*

Sum of the HTTP-sites, blocked by *Virus Protection*

Using the Security System

5.8.7. PPTP/IPSec VPN

The PPTP and IPSec-VPN connections will be displayed in a graphic in this menu.

5.8.8. Intrusion Protection

Intrusion Protection events will be displayed in a graphic in this menu.

5.8.9. DNS

The DNS-Query-statistic is represented in this menu.

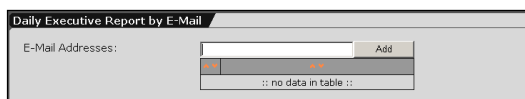
5.8.10. HTTP Proxy Usage

The access to the **HTTP-Proxy** is recorded in this menu.

5.8.11. Executive Report

In the **Executive Report** menu, a complete report is created from the individual reports in the **Reporting** tab.

Daily Executive Report by E-Mail



The screenshot shows a window titled "Daily Executive Report by E-Mail". Inside, there is a label "E-Mail Addresses:" followed by a text input field. To the right of the input field is a button labeled "Add". Below the input field is a table with a single row containing the text "no data in table".

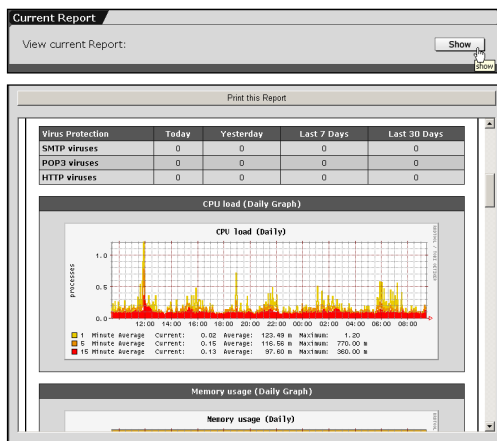
Once a day an updated complete report is sent to the e-mail addresses entered into the **ordered list**.

The function is automatically enabled, once an address has been entered into the field.

New e-mail addresses are taken over to the ordered list by the entry field, by clicking on the **Add** button.

Ordered Lists are described in chapter 4.3.4 on page 39.

Current Report



Clicking on the **Show** button opens a window, in which the current complete report is displayed. This report can be printed out by clicking on the **Print this Report** button.

5.8.12. Accounting

The 'Generate Accounting Reports' window displays the following configuration:

- Status: ☒ (Disable button)
- Accounting Report Type: Full
- Queried Networks:
 - Selected: Internal (Network)
 - Available: Any, Bookkeeping, Development, FTP Server, Internal (Address)

The **Accounting** function monitors all IP packets, transmitted over the various network cards and, once a day, summarizes their size.

Statistics for the preceding month are also generated at the beginning of each new month. These statistics are then used to generate a report. This report is useful, for instance, when an organization pays its service provider based on the volume of data transmitted.

Accounting is configured and enabled in the **Network/Accounting** menu. Further information is available in chapter 5.3.7 on page 175.

Browse Accounting Reports: The existing accounting protocols will be displayed in this window. Select the month from the **Select Report** drop-down menu. The report will appear in the window below.

Using the Security System

Use the **Local Logs/Browse** menu to download or delete reports.

Report for current Month: This window displays the accounting report for the current month.

Configuring Accounting:

1. Under the **Reporting** tab, select the **Accounting** menu.
2. Enable the **Accounting Reports** subsystem by clicking the **Enable** button.

The entry window will open.

3. Use the selection field in the **Queried networks** window to select the networks for which detailed reports should be generated. This will usually include your LAN and/or DMZ networks.

Please see chapter 4.3.2 on page 36 for a description of how to use **selection fields**.

Important Note:

Do NOT use the "Any" network, since it will match all source and destination networks, meaning no traffic will be counted in the report!

The changes will be applied immediately, and the networks will appear in the **Queried networks** window.

5.8.13. System Information



This menu offers additional system information. This information will be displayed in a separate window. Clicking on the **Show** button opens this window.

Filesystem	IF-blocks	Used	Available
rootfs	608756	307336	274096 53%
/var/croot	608756	307336	274096 53%
tmpfs	32768	3284	29484 11% /var/tmpfs
/dev/hda1	350007	80398	136845 5% /boot
/dev/hda2	4484560	204764	1387466 2% /var/crootage
/dev/hda3	350007	8239	349168 2% /var/cupdate
/dev/hda4	350007	231242	144889 6% /var/sec
/dev/hda5	19823468	97580	18748560 1% /var/log
/dev/hda6	917104	16580	890524 1% /var/c
none	128240	0	128240 0% /var/sha

Disk Partition: This table lists the disk partitions on the system and their usage levels.

[illegible]

Process list: This tree lists all current processes on the Internet security system.

The screenshot shows a Windows command prompt window with the title "[host.domain.com] Interface Information - Microsoft Internet Explorer". The address bar shows "[host.domain.com] Interface Information: [Refresh] Auto refresh (Press F5 to refresh manually)".

The command prompt displays the following output:

```
eth0
Link encap:Ethernet HWaddr 00:0C:0E:D6:23:3F
inet addr:192.168.0.17 Bcast:192.168.0.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST  MTU:16384 Metric:1
RX packets:57108 error:0 dropped:0 overruns:0 frame:0
TX packets:110137 error:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:540465 (5.2 Mb)  TX bytes:1864616 (17.7 Mb)
Interrupt:5 Base address:0xc8000

io
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
UP LOOPBACK RUNNING  MTU:16384 Metric:1
RX packets:6504559 error:0 dropped:0 overruns:0 frame:0
TX packets:6504559 error:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:100
RX bytes:46581897 (44.6 Mb)  TX bytes:46581897 (44.6 Mb)
Interrupt:9 Base address:0
```

Interface Information: All configured internal and external network cards are listed here.

Using the Security System

ARP Table: This table displays the current ARP cache of the system. It lists all known associations between IP addresses and hardware (MAC) addresses.

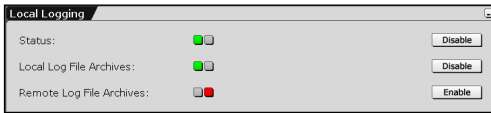
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	127.0.0.1:8001	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:15723	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:1783	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:8080	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:16464	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:80	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:16498	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:53	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN
tcp	0	0	127.0.0.1:8888	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:25	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:443	0.0.0.0:*	LISTEN
tcp	0	0	192.168.5.217:443	10.113.113.21:4393	TIME_WAIT
tcp	0	0	127.0.0.1:16498	127.0.0.1:44289	TIME_WAIT
tcp	0	0	127.0.0.1:16498	127.0.0.1:44353	TIME_WAIT
tcp	0	0	127.0.0.1:16498	127.0.0.1:44322	TIME_WAIT
tcp	0	2824	192.168.5.217:443	10.113.113.21:4395	ESTABLISHED
tcp	0	0	127.0.0.1:16498	127.0.0.1:44292	TIME_WAIT
tcp	0	0	127.0.0.1:16498	127.0.0.1:44276	TIME_WAIT

Local Network Connections: This table lists all current network connections to the firewall. Connections through the firewall are not shown.

5.9. Local Logs (Log Files)

The logs, generated by the system will be managed in the **Local Logs** tab.

5.9.1. Settings



Configure the basic settings for the creation of log files in the **Settings** menu.

Status: Click the **Enable** button to enable the function (status light shows green).

Important Note:

When this function is disabled, the Internet security system will not create **Log Files**!

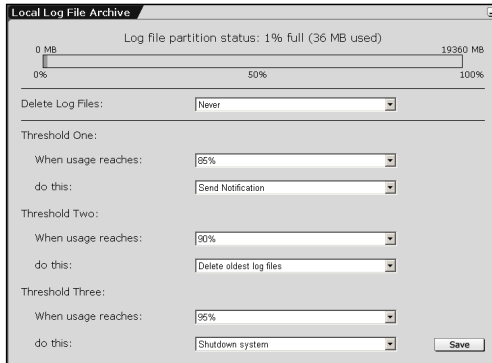
Local Log File Archives: This function locally stores generated log files to the Security system. Configure the settings for the local log file archive in the **Local Log File Archive** window.

By default, this function is enabled automatically, once the logging functions are enabled.

Remote Log File Archives: This function allows you, to save the generated log files to a remote host or server. The settings for the automatization of the log file archive on a separate server are configured in the **Remote Log File Archive**.

Using the Security System

Local Log File Archive



The screenshot shows a window titled "Local Log File Archive". At the top, it displays "Log file partition status: 1% full (36 MB used)" with a progress bar from 0 MB to 19360 MB. Below this, there are three threshold settings:

Threshold	When usage reaches:	do this:
Threshold One:	95%	Send Notification
Threshold Two:	90%	Delete oldest log files
Threshold Three:	95%	Shutdown system

At the bottom right is a "Save" button.

This window allows you to observe the utilization of the local log file partition. The diagram first displays the used disk space in MB as well as the utilization of the partition in percent.

In the lower window, select from the drop-down menu, how the system has to react

if a specific part of the partition is overloaded with log files. Three levels with different actions can be selected here.

Configuring the Log Files Level:

For each level, the following settings can be configured:

When Usage reaches: Configure here, at which utilization in percent of the system partition an action will be executed.

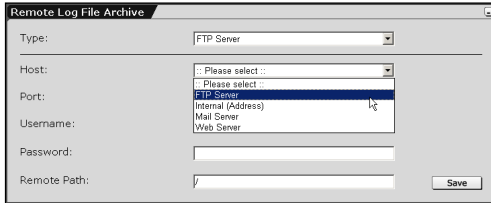
do this: Configure the action in this selection menu.

The following actions can be configured:

- **Delete oldest Log Files:** The oldest log files will automatically be deleted by the Security system. The administrator previously receives the WARN 711 notification e-mail.
- **Send Notification:** Only the INFO 710 notification e-Mail with the correspondent warning will be sent to the administrator.
- **Shut down System:** The security system will automatically shut-down. The administrator receives the CRIT 712 notification e-Mail before.
- **Nothing:** No actions will be started.

Save the settings by clicking on the **Save** button.

Remote Log File Archive



The screenshot shows a window titled "Remote Log File Archive". It contains several fields and dropdown menus: "Type:" with a dropdown menu showing "FTP Server"; "Host:" with a dropdown menu showing "Please select ::"; "Port:" with a dropdown menu showing "Please select ::" and a list of options including "FTP Server", "Internal (Address)", "Mail Server", and "Web Server"; "Username:" with a text entry field; "Password:" with a text entry field; and "Remote Path:" with a text entry field. A "Save" button is located at the bottom right of the window.

In this window configure the settings for a remote log files archive. If the *Remote Log File Archive* is on a server, you must first add it to the **Definitions/Networks** menu.

Configuring Remote Log File Archive:

1. In the **Global Settings** window, enable the **Remote Log File Archives** function by clicking on the **Enable** button.

The **Remote Log File Archive** window will open.

2. Use the **Type** drop-down menu to select the archiving type.

The drop-down menus and/or entry fields for the selected archiving type will be displayed.

3. Configure the settings for the archiving type.

3.1 FTP Server

Host: Use the drop-down menu to select a host.

Port: Use the drop-down menu to select a port.
By default, FTP is already selected.

Username: Enter a username in the entry field.

Password: Enter the password in this entry field.

Remote Path: Enter the path in the entry field.

Using the Security System

3.2 SMB (CIFS) Share

Host: Use the drop-down menu to select a host.

Username: Enter a username in the entry field.

Password: Enter the password in this entry field.

Share Name: Enter the share name in the entry field.

3.3 Secure Copy (SSH) Server

Public DSA Key: The Public DSA Key is displayed in this window.

Host: Use the drop-down menu to select a host.

Username: Enter a username in the entry field.

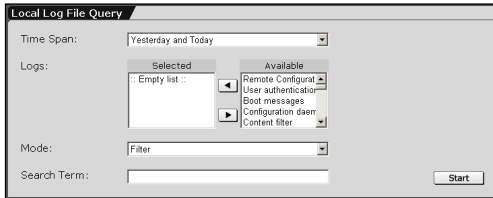
Remote Path: Enter the absolute path in the entry field.

3.4 Send by E-Mail

E-Mail Address: Enter the e-Mail address into this entry field.

4. Save your changes by clicking **Save**.

5.9.2. Local Log File Query



The **Local Log File Query** action allows you, to search for specific **Log Files** in a local archive. The search result will be displayed in a separate window.

Starting searches:

1. In the **Time Span** drop-down menu select the time span.
2. In the selection field **Logs**, choose the protocols.
Please see chapter 4.3.2 on page 36 for a description of how to use **selection fields**.
3. In the **Mode** drop-down menu, select the mode.
4. If you are looking for protocols with specific strings, enter the strings into the **Search Term** entry field.
5. Begin the search by clicking **seek**.

The protocols will be listed in a separate window.




























































Using the Security System

5.9.3. Browse

Each protocol is contained in the **Browse** menu. If this menu is opened, the protocol groups (logs) will be displayed in the **Browse Local Log Files** overview.

The Log File Overview

All protocol groups (logs) are contained in this overview. The groups with the current protocols can directly be opened from this overview.


Browse local Log Files (show support logs)						
Total 121 entries, 102 filtered				▽ Filters ▾		
	▽ Name	Date	File Count/Name	Activity	Size	
	Accounting data		 4 files		184	
	Admin notifications		 6 files	Today	3064	
	Boot messages		 6 files		3473	
	Content filter		 4 files		254	
	DHCP server		 4 files		383	
	DNS proxy		 6 files	Today	39kB	
	HTTP proxy		 4 files		5669	
	Intrusion Protection System		 4 files		657kB	
	Kernel messages		 6 files	Today	82kB	
	Local logins		 6 files		1240	
	Logging subsystem		 6 files	Today	1462	
	Packet filter		 6 files	Now	126kB	
	PPTP daemon		 4 files		227	
	Selfmonitoring		 6 files		80kB	
	SMTP proxy		 6 files	Today	132kB	
	SSH daemon		 6 files		269	
	System log messages		 6 files	Today	27kB	
	User authentication daemon		 6 files	Today	1439	
	WebAdmin		 6 files	Now	23kB	
checked entries: :: Please select :: ▾						

The functions from the left to the right:

Selection box: This setting is required in connection with the drop-down menu at the footer of the table. Select the protocol groups and then choose the action (**Delete** or **Download as ZIP File**) from the drop-down menu.


The action will start immediately.

Clicking on the selection box in the header selects all protocol groups.

(): Clicking on the trash can icon deletes a group from the table.

Name: All protocols are listed in alphabetical order in this column.

Date: The date of current protocols will not be displayed.

(): Clicking on the folder icon opens the sub-tab with all protocols of this group.

By clicking again on the icon, you will get back to the overview. The additional functions in the sub-tab are described in the „Log File Sub-tab“ section.


File Count/Name: The number of existing files will be displayed in this column. The old protocols can be opened from the sub-tab.

Activity: If the protocols in a group have been logged since Midnight, a correspondent message will be displayed:

- **Now:** The protocols are being generated right now.
- **Today:** Protocols have been generated since Midnight.


Open the protocols by clicking on the message Now or Today. Open the current protocol (**Live Log**) by clicking on the message **Now** or **Today** (see left-hand picture).














Size: The size of the log file group will be displayed in this column.























(): Clicking the download icon will allow you to download this **Log File** to your local client computer. You can then use these **Log Files** to import data into another program, for example Microsoft Excel.

Using the Security System

The Log File Sub-Tab


All protocols (Logs) of a group are listed in this sub-tab. The sub-group can be opened in the overview by clicking on the folder icon ()

Browse local Log Files (show support logs)		Total 121 entries, 102 filtered		▽ Filters ▽	
	▽ Name	Date	File Count/Name	Activity	Size
	Accounting data		 4 files		184 
	Admin notifications		 6 files	Today	3064 
	Boot messages		 6 files		3473 
	Content filter		 4 files		254 


Browse local Log Files (show support logs)		Total 121 entries, 114 filtered		▽ Filters ▽	
	▽ Name	Date	File Count/Name	Activity	Size
	Admin notifications		 6 files	Today	3064 
	Admin notifications	Tuesday April 06 2004	 /var/log/notifier.log (Live log)	Today	225 
	Admin notifications	Monday April 05 2004	 notifier-2004-04-05.log.gz		515 
	Admin notifications	Sunday April 04 2004	 notifier-2004-04-04.log.gz		784 
	Admin notifications	Saturday April 03 2004	 notifier-2004-04-03.log.gz		644 
	Admin notifications	Friday April 02 2004	 notifier-2004-04-02.log.gz		457 
	Admin notifications	Thursday April 01 2004	 notifier-2004-04-01.log.gz		439 
checked entries: <input type="text" value=":: Please select ::"/>					

The following additional functions are available in the sub-tab:

Date: For older protocols, listed in the sub-tab the date and time will be displayed.

(): Return to the overview by clicking on the folder icon.

(): This is today's protocol. Clicking on the icon opens the **Live Log** window.

(): This is an archived protocol. Clicking on the symbol opens the **Log** window.

File Count/Name: In the protocol from today, the path to the log file and the **Live Log** message will be displayed in this column.

In this column, the file names will be displayed next to the archived log files.

Filters

The **Filters** function allows you to filter *Log Files* with specific attributes from the table. This function enhances the management of huge networks, as log files of a specific type can be presented in a concise form.

Filtering Log files:

1. Click on the **Filters** button.

The entry window will open.

2. Enter the filter attributes in the fields. Not all attributes have to be defined.

Group: If you wish to filter the log files of a specific group, select it from the drop-down menu.

Month: This drop-down menu allows you to filter log files by a given month.

Type: This drop-down menu allows you to filter log files by a specific type.

3. To start the filter click on the **Apply Filters** button.

Only the filtered log files will be displayed in the table. Next time when you open the menu, the complete log file table will be displayed.

Using the Security System

5.9.3.1. Log Files

This chapter contains all available logs. These log files will only be displayed in the **Browse** menu, if the correspondent processes have been recorded by the System. The following **Accounting data** log file, for example, will only be displayed, once the **Accounting** function has been enabled in the **Network/Accounting** menu.

Accounting data: These log files contain all **Accounting** logs, archived by the system. The **Reporting/Accounting** menu allows you to view the current logs.

Astaro Configuration Manager: If the Internet security system is configured remotely via the Astaro Configuration Manager, the correspondent processes will be logged to these log files.

Astaro User Authentication: The activities of the AUA Daemon are logged to these log files. AUA is used as the central authentication daemon for various services.

Boot messages: The boot messages are recorded to these log files.

Configuration daemon: The activities of the AUA Daemon are logged to these log files. The log files belong to the support logs and will only be displayed after clicking on the **show support logs** button.

Content Filter: The activities of the content filters on the HTTP, SMTP and POP3 Proxies are logged to these log files.

DHCP client: If the interfaces are automatically assigned to IP-addresses on the Internet security system, the activities are recorded to these log files.

DHCP server: If the Internet security system is used as DHCP-server and assigns dynamic IP addresses to the clients in the network, the activities are recorded to these log files.

Fallback archive: These log files are used as a security archive for logged processes, which cannot be assigned to one of the log files.

Using the Security System

The log files belong to the support logs and will only be displayed after clicking on the **show support logs** button. In general, those log files are empty.

High Availability: The activities of the **High-Availability-(HA)** system are logged to these log files.

HTTP daemon: The log files for the HTTP daemon belong to the support logs and will only be displayed after clicking on the **show support logs** button.

WebAdmin access: The requests to the user data base are recorded to these log files.

Intrusion Protection: The activities of the **Intrusion Protection System (IPS)** are recorded to these log files.

IPSec VPN: Extensive information on the configuration of the **IPSec-VPN** and **L2TP-over-IPSec**-connections is recorded to these log files. And also information on the Key Exchange and Encryption.

Virus Protection: The activities of the **Virus Protection System** are recorded to these log files.

Kernel: The **Kernel** logs record the system status, including messages from device drivers, messages relating to the boot process, and information about blocked packets.

Logging: The local archives of the log files on the Internet security system and the forwarding of files to the *Remote-Log-File-Archive* are recorded to these log files.

Local login: Information on the log-in processes to the local console is recorded to these log files.

MiddleWare: The activities of the MiddleWare are recorded to these log files. The log files belong to the support logs and will only be displayed after clicking on the **show support logs** button.

Network accounting daemon: The efficiency of the accounting is recorded to these log files.

Using the Security System

BIND name server: The releases of host names to IP-addresses are recorded to these log files.

Admin notifications: The **Notification Log Files** record all notification e-mails sent by the firewall. This allows an administrator to monitor critical system messages even if the e-mail system is down.

Error, warning, and information codes are listed in chapter 5.9.3.2 on page 320.

HTTP proxy: The **HTTP proxy** logs show the activity of the HTTP proxy.

Packet Filter: Messages relating to blocked packets are shown in the **Packet Filter** logs. These log files are also included in the kernel logs.

POP3 proxy: The activities of the POP3-Proxy are logged to these log files. All outgoing e-Mails will be listed there. In addition, all irregularities, such as interruptions or blocked e-mails will be logged.

Portscan Detection: The *Portscan Detection* system watches for and blocks portscans and sends e-mail messages to the administrator. When examining the **Log Files**, however, do not draw too many conclusions from the source IP addresses (SRC) and port numbers (SPT), as they can easily be falsified by the sender. The destination addresses (DST) and port numbers (DPT), however, provide useful information about what the scanner was looking for.

PPPoA DSL dial-up: The processes executed in the dial-up with *PPP over ATM* are recorded to these log files.

PPPoA DSL dial-up: The processes executed in the dial-up with *PPP over Ethernet* are recorded to these log files.

PPTP VPN Access: These logs record the progress of PPTP sessions from external clients. This includes login and authentication information as well as error messages.

If you select the **Extensive** parameter in the **Logging** function of the **Network/PPTP VPN Access** menu, these logs will contain very detailed information about PPP connections.

Self-monitor: The **Self-monitoring** continually checks the integrity of the firewall systems and notifies the administrator of important events. Self-monitoring checks the function, performance and security of relevant system parameters and remedies deviations, exceeding given tolerances. Subsequently a report will be sent to the competent administrator by e-mail.

This **Self-monitoring** of the security system ensures that central services such as the Syslog Daemon, HTTP Proxy, and Network Accounting are functioning properly.

Access rights to files are monitored, as is the resource usage of individual processes. This is designed to prevent an overload of the system. Moreover, the system administrator is informed in time on previsible resource bottlenecks, if, for example the available disk space is running short. This allows for an early implementation of measures in favor of a system extension and/or discharge.

SMTP proxy: The activities of the SMTP-proxy are recorded to these log files. All ingoing e-Mails will be listed there. In addition, all irregularities, such as assigned **Bounce** conditions, interruptions or blocked e-mails will be logged.

SOCKS proxy: The activities of the SOCKS-proxy are recorded to these log files.

SSH remote login: Information on the log-in processes to the remote shell is recorded to these log files.

System log messages: These **Log Files** record generic information about the daemon processes running on the system. Among other things, the access to the **SNMP**-service and the activities of the **Dynamic DNS** function, are recorded to these log files.

Using the Security System

Up2Date Service messages: The activities of the **Up2Date Service** are recorded to these log files. This comprises also the *System Up2Date* and *Pattern Up2Date* processes.

Uplink Failover messages: The activities of the configured failovers are recorded to these log files.

WebAdmin usage: The use of the **WebAdmin** configuration tool is recorded to these log files. The logs contain the configuration changes, implemented by the configuration tool and also the log-in and log-out processes.

5.9.3.2. Error Codes

The following is a list of all error, warning, and information codes with their meanings:

INFO:

000	System was restarted
	System was restarted
010	Backup file
	A system backup file was generated automatically and sent via e-mail to the Administrator.
105	Astaro User Authenticator (AUA) not running - restarted
106	Cron Task Scheduler not running - restarted
107	WebAdmin webserver not running - restarted
108	ssh server not running - restarted
109	license server not running - restarted
110	configuration database server not running - restarted
111	syslog server not running - restarted

Using the Security System

112 middleware not running - restarted

150 Root partition mounted at / is filling up -
 please check

151 tmpfs partition mounted at /opt/tmpfs is filling
 up - please check

152 secure application partition mounted at /var/sec
 is filling up - please check

153 logfile partition mounted at /var/log is filling
 up - please check

154 storage application partition mounted at
 /var/storage is filling up - please check

155 Up2Date partition mounted at /var/up2date is
 filling up - please check

300 System Up2Date: System Up2Date started

 Further information on the Up2Date Service can
 be found in chapters 5.1.3 on page 54.

302 System Up2Date: No new System Up2Date packages
 available

303 System Up2Date succeeded: Prefetched new System
 Up2Date package(s)

 For more Up2Date package information please see
 attached Up2Date description file.

 Further information on the System Up2Date can be
 found in chapters 5.1.3 on page 54.

320 System Up2Date failed: License is not valid

321 System Up2Date: Started System Up2Date install-
 lation in HA-Master-Mode

322 System Up2Date: New System Up2Dates installed

Using the Security System

Further information on the Up2Date package(s) can be found in the notification e-mail.

323 System Up2Date: Started System Up2Date Installation

350 Pattern Up2Date: Started Pattern Up2Date

Further information on the Up2Date Service can be found in chapters 5.1.3 on page 54.

351 Pattern Up2Date: No new pattern available for Virus Protection

352 Pattern Up2Date: No new pattern available for Intrusion Protection

353 Pattern Up2Date: Trying another pattern type

354 Pattern Up2Date succeeded: Updated new Intrusion Protection patterns

For more information please see the notification e-mail. Further information on the System Up2Date can be found in chapters 5.1.3 on page 54.

360 Virus Pattern Up2Date: No pattern installation for Virus pattern needed

361 Virus Pattern Up2Date succeeded: Installed new Virus Pattern

For more information please see the notification e-mail.

700 Daily log file archive

This is an archive file containing the log files. The date of these log files is specified in the notification.

710 Log file partition is filling up

Using the Security System

The log file partition usage reached the specified value in percent. Depending on your configuration the system will automatically take measures if the usage continues to grow. To make sure you don't lose any important log files, please check the WebAdmin settings and/or remove old log files manually.

850 Intrusion Protection Event

A packet was identified that may be part of an intrusion. The matching rule classified this as low priority level. Further information on the Intrusion Prevention event can be found in the notification e-mail.

851 Intrusion Protection Event - Event buffering activated

A packet was identified that may be part of an intrusion. The matching rule classified this as low priority level. Event buffering has been activated. Further Intrusion Protection events will be collected and sent to you when the collection period has expired. If more events occur, this period will be increased. Further information on the Intrusion Prevention event can be found in the notification e-mail.

855 Portscan detected

A portscan was detected. The originating host was: <IP>

A portscan from the given IP address was detected. The Portscan Detection Module is described in chapter 5.4.1, on page 179.

For more information:

- see WebAdmin -> Local Logs/Browse/Portscan

Using the Security System

- search with whois to know who the source IP belongs to:
- > RIPE NCC [http://www.ripe.net/perl/whois?query=\\$HOST](http://www.ripe.net/perl/whois?query=$HOST)
- > ARIN - [http://www.arin.net/cgi-bin/whois.pl?queryinput=\\$HOST](http://www.arin.net/cgi-bin/whois.pl?queryinput=$HOST)
- > APNIC - [http://cgi.apnic.net/apnic-bin/whois.pl?search=\\$HOST](http://cgi.apnic.net/apnic-bin/whois.pl?search=$HOST)
- use traceroute from
- > UC Berkeley
- [http://www.net.berkeley.edu/cgi-bin/traceroute? \\$HOST](http://www.net.berkeley.edu/cgi-bin/traceroute? $HOST)

Attention: source IP addresses can easily be forged by attackers.

856 Portscan detected - Event buffering activated

A portscan was detected. The originating host was: <IP>

A portscan from the given IP address was detected. The Portscan Detection Module is described in chapter 5.4.1, on page 179.

Event buffering has been activated. Further Intrusion Protection events will be collected and sent to you when the collection period has expired. If more events occur, this period will be increased. Further information on the Intrusion Prevention event can be found in the notification e-mail.

999 File transfer request

This is the file you requested.

Using the Security System

WARN:

001 A feature will expire! The feature ... is time limited and will expire in ...

Please contact your local Astaro partner or an Astaro sales representative to obtain a license update.

E-Mail addresses:

America's: <mailto:salesus@astaro.com>,

Europe, Asia Pacific and Africa:

<mailto:sales@astaro.com>.

For technical questions, please feel free to visit our user bulletin board at <http://www.astaro.org>, or our documentation resources at <http://docs.astaro.org>.

005 Failed login attempt from ...(IP) at ...(time) with ...(username)

080 HA check: no link beat on interface - retrying

The link beat monitoring system on the firewall failed. The system will now try again. If the system continues to fail, the administrator will receive message WAR 081.

If you do not wish to use this monitoring function, no further action is required. After the system sends the WAR 081 message, it will not try to start the link beat monitoring system again.

081 HA check: interface does not support link beat check

The link beat monitoring system failed after multiple attempts. If you have recently installed the HA system, and you intend to use the

Using the Security System

link beat monitoring system, please check that the network cards support link beat, and that they are supported by the security system. Also check to make sure that the link beat capable cards have been chosen for the data transfer connection.

The installation and management of the HA system is described in chapter 5.1.10, on page 97.

711 Log file(s) have been deleted

The log file partition usage reached the specified value in percent. Log Files have been deleted. To make sure you don't lose more log file(s), please check the WebAdmin settings and/or remove old log files manually. The deleted files and/or directories are listed in the attachment.

715 Remote log file storage failed

The daily log file archive could not be stored on the configured remote server. Please check the WebAdmin settings for:

Local Logs/Settings/Remote log file archive

The archive file will be automatically re-transferred with the next daily log file archive.

850 Intrusion Protection Event

A packet was identified that may be part of an intrusion. The matching rule classified this as medium priority level. Further information on the Intrusion Prevention event can be found in the notification e-mail.

851 Intrusion Protection Event - Event buffering activated

Using the Security System

A packet was identified that may be part of an intrusion. The matching rule classified this as medium priority level. Event buffering has been activated. Further Intrusion Protection events will be collected and sent to you when the collection period has expired. If more events occur, this period will be increased. Further information on the Intrusion Prevention event can be found in the notification e-mail.

CRIT:

301 System Up2Date failed: Could not connect to Authentication Server(s)

The authentication server is not reachable. If the problem continues, please contact the support department of your firewall provider.

302 System Up2Date failed: Download of System Up2Date Packages failed

If the problem continues, please contact the support department of your firewall provider.

305 System Up2Date: Wrong MD5sum for local System Up2Date package

Please download a new Up2Date package. The Up2Date packages can be downloaded from <http://download.astaro.de/asl/up2date>. If the problem recurs, please contact the support department of your firewall provider.

306 System Up2Date failed: Wrong MD5sum for downloaded Up2Date Package

Please download a new Up2Date package. If the problem recurs, please contact the support department of your firewall provider.

Using the Security System

- 320 System Up2Date failed: Wrong start parameters
 If the problem recurs, please contact the support department of your firewall provider.
- 322 System Up2date stopped: Next Up2Date installation locked by HA
- 323 System Up2Date failed: Corrupt Up2Date Package
 Found corrupt Up2Date package. Please start process again. If the problem recurs, please contact the support department of your firewall provider.
- 324 System Up2Date failed: Invalid License
 Your license is no longer valid.
- 325 System Up2Date failed: License check failed
 Your license could not be checked. If the problem continues, please contact the support department of your firewall provider.
- 333 System Up2Date failed: Internal error
 The system update failed. Please contact the support department of your firewall provider.
- 334 System Up2Date failed: Invalid syntax
 The system update failed. Please contact the support department of your firewall provider.
- 335 System Up2Date failed: Could not read Up2Date directory
 The system update failed. Please contact the support department of your firewall provider.
- 336 System Up2Date failed: No installation directory
 The system update failed. Please contact the support department of your firewall provider.

Using the Security System

- 337 System Up2Date failed: Could not extract tar
Please start process again. If the problem
recurs, please contact the support department of
your firewall provider.
- 338 System Up2Date failed: Main Up2Date package not
found
Please start process again. If the problem
recurs, please contact the support department of
your firewall provider.
- 339 System Up2Date failed: Version conflict
The system update failed. Please contact the
support department of your firewall provider.
- 340 System Up2Date failed: Pre-Stop-Services script
failed
- 341 System Up2Date failed: Post-Stop-Services script
failed
- 342 System Up2Date failed: Pre-Start-Services script
failed
- 343 System Up2Date failed: Starting Services failed
The system update failed. Please contact the
support department of your firewall provider.
- 344 System Up2Date failed: Post-Start-Services
script failed
- 345 System Up2Date failed: Error occurred while
running installer
The system update failed. Please contact the
support department of your firewall provider.
- 346 System Up2Date failed: Installer ended due to
internal error

Using the Security System

The system update failed. Please contact the support department of your firewall provider.

347 System Up2Date failed: Started without rpm parameters

The system update failed. Please contact the support department of your firewall provider.

351 Pattern Up2Date failed: Could not select Authentication Server(s)

If the problem continues, please contact the support department of your firewall provider.

352 Pattern Up2Date failed: Could not connect to Authentication Server(s)

The authentication server is not reachable. If the problem continues, please contact the support department of your firewall provider.

353 Virus Pattern Up2Date failed: Could not connect to Up2Date Server

The Up2Date server is not reachable. If the problem continues, please contact the support department of your firewall provider.

354 Intrusion Protection Pattern Up2Date failed: Could not connect to Up2Date Server

The Up2Date server is not reachable. If the problem continues, please contact the support department of your firewall provider.

355 Virus Pattern Up2Date failed: No active bases for Virus Patterns found

356 Intrusion Protection Pattern Up2Date failed: No active bases for Intrusion Protection Patterns found

Using the Security System

357 Virus Pattern Up2Date failed: Internal MD5Sum Error

Could not create correct MD5Sums. If the problem recurs, please contact the support department of your firewall provider.

358 Intrusion Protection Pattern Up2Date failed: Internal MD5Sum Error

Could not create correct MD5Sums. If the problem recurs, please contact the support department of your firewall provider.

360 Pattern Up2Date failed: Licence Check failed

Your license could not be checked. If the problem continues, please contact the support department of your firewall provider.

361 Pattern Up2Date failed: Restart of Virus Scanner failed

If the problem continues, please contact the support department of your firewall provider.

362 Pattern Up2Date failed: MD5Sum Error occurred

If the problem continues, please contact the support department of your firewall provider.

712 System shut down due to full log file partition

The log file partition usage reached the specified value in percent. To prevent the loss of important log files, the system has been shut down automatically. Please check the WebAdmin settings and/or remove old log files.

850 Intrusion Protection Event

A packet was identified that may be part of an intrusion. The matching rule classified this as

Using the Security System

highest priority level. Further information on the Intrusion Prevention event can be found in the notification e-mail.

851 Intrusion Protection Event - Event buffering activated

A packet was identified that may be part of an intrusion. The matching rule classified this as highest priority level. Event buffering has been activated. Further Intrusion Protection events will be collected and sent to you when the collection period has expired. If more events occur, this period will be increased. Further information on the Intrusion Prevention event can be found in the notification e-mail.

860 Intrusion Protection Event - Buffered Events

After the activation of the event buffering further IPS events have been collected. Please see the attached file for a list of collected events. This list will show you a maximum of events. A complete event history has been stored in the Intrusion Protection log files.

5.10. Online Help

The **Help** menu contains further functions for use with the **Online Help** system.

Search

This function allows you to search **WebAdmin's Online Help** system for a particular term. Results will appear in a separate window.

Starting a search:

1. Under the **Online Help** tab, open the **Search** menu.
2. Enter your search term in the **Search term** field.
3. Begin the search by clicking **seek**.

If the term is found in either **WebAdmin** or the **Online Help** system, the following results will be returned:

- path to the relevant function in **WebAdmin**
- link to the relevant **Online Help** page
- Information on the function or texts of the Online help with the expression, searched for

Glossary

The glossary explains the concepts and terms used in **WebAdmin**. Click a term to see a short explanation.

5.11. Exiting the Security Solution

If you close a browser running a **WebAdmin** session without using the **Exit** function, the session will remain active until the timeout is reached.

In such a case you can again log in to **WebAdmin**. A screen will be displayed, informing you that already another user is logged in. To log in again, first end the other session by clicking the **Kick** button. If you wish to end another administrator's active session, you can type a message in the "Type reason here" field which will be transmitted to the other administrator.

Glossary

Broadcast

The address used by a computer to send a message to all other computers on the network at the same time.

Example: A network with address 212.6.145.0 and netmask 255.255.255.240 would have a broadcast address of 212.6.145.15.

Client

A client is a program that communicates over a network with a server in order to make use of a particular service.

Example: Netscape is a WWW client, and communicates with a WWW server to download web pages.

Client-Server model

Applications based on the client-server model use a client program on the user's computer to communicate with a central server program on the network. The server is usually responsible for keeping track of the data, while the client is responsible for presenting the data to the user. In order to function correctly, the client and server must both use a well-defined network protocol to communicate. All important applications on the Internet (e.g. WWW, FTP, news) use this model.

DNS

The Domain Name Systems (also: The Domain Name Service) translates the underlying IP addresses of Internet-connected computers into more human-friendly names or aliases and vice-versa. This translation from number to name is done by the name server. Every Internet-connected institution must employ at least two separate DNS servers to answer queries about its internal DNS names

Glossary

and IP numbers. Every top-level domain also has name servers which contain information about their subordinate servers.

The DNS system is thus a distributed, hierarchical database. DNS resolution is normally handled by network applications rather than by the user him or herself.

Dual-Homed Gateway

A dual-homed gateway is a computer that is directly connected to two networks (i.e., it has two network cards, each connected to a different network) and which forwards information from one network to the other. Due to the fact that there is no IP forwarding, all connections must be forwarded through this Dual-Homed Gateway.

Firewall

A firewall protects one network or subnet (e.g., an internal LAN) from another network (e.g., the public Internet). All traffic between the two passes through the firewall, where it is controlled and monitored.

Header

In general, the header is the information contained at the top of a file or message, and consists of low-level data regarding the status and handling of the file or message. In particular, the header of an e-mail or Usenet message contains information such as the sender, recipient, and date.

Host

In a client-server architecture, the host is the computer which runs the server software. One host can have multiple server programs running on it: that is, an FTP server, mail server, and web server can all run on the same host. A user uses a client program, for instance a browser, to access the server on the host. The word **Server** is also

often used to refer to the computer on which the server software runs, diluting the distinction between server and host in practice.

In telecommunications, the host is the computer from which information (such as FTP files, news, or WWW pages) is retrieved. On the Internet, hosts are often also called **nodes**.

Using an Internet host (as opposed to a **Localhost**), for example with Telnet, one can work from a distance (Remote Access).

ICMP

Next to the **IP Protocol**, there is an option with specific functions. The **Internet Control Message Protocol (ICMP)** is a special kind of **IP protocol** used to send and receive information about the network's status and other control information. Many users are already familiar with ICMP echo requests (type 8) and echo replies (type 0), as these are used by the **ping** program. When a computer receives an echo request, its IP stack sends back an echo reply: This is done with the ping program in order to determine, whether another network component is reachable.

IP

The **Internet Protocol** is the basic protocol of the Internet, and has been used without change since it was first developed in 1974. It handles the basic transmission of data from one computer to another, and serves as the basis for higher-level protocols like TCP and UDP. It handles the connection and error management. Technologies like **NAT** and **Masquerading** allow large private networks to hide behind small numbers of IP addresses (or even single addresses), thus allowing the relatively limited IPv4 address space to meet the demands of an ever-expanding Internet.

Glossary

IP-Address

Every (publicly-addressable) host on the Internet has a unique IP address, similar to a telephone number. An IP address consists of decimal numbers, separated by points. Possible numbers are 0 to 255 inclusive.

Example: a possible IP address is 212.6.145.1.

At least one IP name in the form `hostname[.subdomain[s]].domain`, z. B. `kises.rz.uni-konstanz.de` is assigned to an IP address. This refers to a computer, named `kises`, which stands in the sub-domain `rz` of the sub-domain `uni-konstanz` of the `de` domain. As with IP addresses, the individual parts of the name are separated from each other by a point. Whereas, in contrast to IP-addresses, IP-names are not limited to four numbers. Moreover, several IP-names can be assigned to one IP-address, which are referred to as aliases.

Masquerading

Dynamic **Masquerading** is a technology based on NAT that allows an entire LAN to use one public IP address to communicate with the rest of the Internet.

Example: The administrator has established an internal LAN, and has given each computer on it IP addresses from the private IP range 10.x.x.x. One computer, for example, has the address 10.1.2.3. Only one, official IP address is assigned to all computers in its network, i.e. if only one HTTP request starts to the Internet, its IP address will be replaced by the IP address of the external network card.

The data traffic for the external network (Internet) thus does not contain internal information. The answer to the request will be recognized by the firewall and forwarded to the requesting computer.

nslookup

Nslookup is originally a UNIX program designed to query name servers. The main application is the display of IP names in the case of a given IP number and vice versa. Moreover also additional functions, such as aliases can be displayed.

Port

While at the IP level, only sender and destination addresses are important, the TCP and UDP protocols both include the concept of ports. A port is an additional identifier – in the cases of TCP and UDP, a number between 0 and 65535 – that allows a computer to distinguish between multiple concurrent connections between the same two computers. TCP and UDP packets have both a sending port and a destination port.

Protocol

A protocol is a well-defined and standardized set of rules that govern how a client and server interact. Some well-known protocols and their associated services include HTTP (WWW), FTP (FTP), and NNTP (news).

Proxy (Application Gateway)

Proxies, often called application gateways, separate two networks at the network (IP or TCP/UDP) level, while still allowing certain kinds of communication. There can be no direct connection between an internal system and an external computer.

Proxies exclusively operation the application level. Proxies-based firewalls use a Dual-Homed Gateway that does not forward IP packets. Proxies, operated as specialized programs on the gateway, can now receive connections for a specific protocol, treat the transmitted traffic on the application level and forward it afterwards.

Glossary

RADIUS

RADIUS stands for Remote Authentication Dial In User Service. It is a protocol designed to allow network devices such as routers to authenticate users against a central database.

Router (Gateway)

A router is a network device that is designed to forward packets to their destination along the most efficient path. Strictly speaking, a gateway is not always a router (it could be an application gateway, or proxy) – though a router is a kind of circuit-level gateway. When a computer wants to communicate with a server not on the local network, it must pass the data to a router in order for the packets to be forwarded to their destination: By convention, the highest or lowest address in the network range is used for the router: for example, in the network 192.168.179.0/24, the router will normally be at either 192.168.179.254 or 192.168.179.1.

Server

A server is a network-connected computer that offers services to client computers. Standard services include WWW, FTP, news, and so on. In order to make use of these services, the user will need a client program (e.g., Netscape) to communicate with the server.

SOCKS

SOCKS is a proxy protocol that allows a point-to-point connection between an internal and an external computer. SOCKS, often called the Firewall Traversal Protocol, is currently at version 5 and must be implemented in the client-side program in order to function correctly.

Subnet Mask

The subnet mask (also called netmask) of a network, together with the network address, defines which addresses are part of the local network and which are not. Individual computers will be assigned to a network on the basis of the definition.

UNC-Path

The **Universal Naming Convention** path is used primarily by computers running a Microsoft operating system to uniquely designate network resources. UNC paths are usually of the form \\Server\Resource.

Index

- Accounting
 - adding/deleting a network card 176
- Accounting..... 175
- Acoustic signals
 - beep, 5 times..... 102
- Administrator e-mail addresses 44
- Backup
 - editing e-mail addresses. 68
 - encryption of e-mail backup file 66
 - generating e-mail backup file 67
 - introduction 62
 - load 63
 - manual creation 64
- Broadcast
 - Internet-wide..... 198
 - segment-wide 199
- Certificate for WebAdmin
 - installing 95
- Certificate for WebAdmin
 - creating 95
- Connection Tracking Helpers
 - introduction 203
 - loading helper modules. 204
- Connection Tracking Table. 208
- Current System NAT Rules 208
- Current System Packet Filter
 - Rules 208
- DHCP Server
 - assigning DNS servers.. 166
 - configuring 165
 - current IP leasing table 168
 - introduction 165
- DHCP Server
 - static mappings..... 167
- DNS Proxy
 - configuring 228

- DNS Server
 - deleting..... 109
 - editing 109
- DNS servers
 - adding 106
- Dynamic DNS
 - Host defining 119
- Dynamic DNS 118
- Error codes
 - CRIT 327
 - INFO..... 320
 - WARN 325
- Errors
 - causes 123
 - Causes..... 26
- Exit..... 334
- Factory Reset 50
- Firewall Hostname 118
- General System Settings..... 44
- Glossary
 - broadcast 335
 - client 335
 - client-server model 335
 - DNS 335
 - dual-homed gateway.... 336
 - firewall..... 336
 - header 336
 - host..... 336
 - ICMP 337
 - IP 337
 - IP address 338
 - Masquerading 338
 - nslookup 339
 - port..... 339
 - protocol 339
 - proxy..... 339
 - RADIUS..... 340
 - router 340
 - server 340
 - SOCKS..... 340

- subnet mask 341
- UNC path 341
- Glossary 333
- Group
 - deleting..... 109
 - editing 109
- Header 251
- High Availability..... 97
- High Availability System
 - installing 98
- Host
 - adding 104
 - deleting..... 109
 - editing 109
- Hostname 118
- HTTP
 - Surf Protection categories
 - 216
- HTTP Proxy
 - enabling the HTTP proxy
 - 213
 - operation modes 212
 - user authentication mode
 - 212
- HTTP-Proxy
 - advanced 226
 - global settings..... 212
 - standard mode..... 212
 - transparent mode 212
- ICMP
 - firewall forwards ping... 203
 - firewall forwards traceroute
 - 202
 - firewall is ping visible ... 203
 - firewall is traceroute visible
 - 202
 - ICMP Forwarding 200
 - ICMP on firewall 201
 - introduction 200
 - Log ICMP Redirects 201
 - ping on firewall 203
 - ping settings..... 203
 - traceroute from firewall 202
 - traceroute settings..... 201
- Ident
 - forward connections..... 237
 - introduction 237
- Installation
 - configuration..... 27
 - instructions..... 22
 - preparation..... 22
 - software..... 22
- Interfaces
 - adding additional addresses
 - 128
 - additional address on
 - Ethernet interface..... 128
 - configuring a Virtual LAN
 - 142
 - configuring PPPoA-DSL . 151
 - configuring PPPoE-DSL . 146
 - current status 121
 - downlink bandwidth (kbits)
 - 127, 144, 148, 154
 - Ethernet network card.. 124
 - introduction 119
 - introduction 119
 - MTU size 127, 144, 148, 154
 - PPPoE-DSL connection.. 145
 - PPPoE-DSL connections 150
 - Proxy ARP 125
 - QoS status 126, 147
 - QoS Status 143, 153
 - Standard Ethernet interface
 - 124
 - uplink bandwidth (kbits)
 - 126, 144, 148, 154
 - Uplink Failover on Interface
 - 125
 - Virtual LAN 140
 - Wireless LAN..... 130
 - Wireless LAN Security .. 130
- Interfaces
 - determining MAC addresses
 - 133

Index

- hardware overview 122
- Wireless LAN access point
..... 134
- Wireless LAN station 137
- Intrusion Protection
 - global settings..... 179
 - introduction 179
 - notification levels..... 181
 - Portscan Detection..... 179
 - rules..... 182
- IPS rule
 - setting 184
- IPSec user group
 - defining..... 107
- IPSec VPN
 - AH-Protocol 266
 - CA Management 290
 - connections 269
 - global IPSec settings 269
 - introduction 260
 - IPSec..... 264
 - IPSec connections..... 270
 - IPSec modes..... 265
 - IPSec protocols 266
 - IPSec system information
..... 270
 - key management..... 267
 - L2TP over IPSec 288
 - local IPSec X.509 key... 282
 - Local Keys 282
 - manual key distribution 267
 - Policies 277
 - PSK authentication..... 284
 - Remote Keys 285
 - RSA authentication 283
 - Transport mode..... 265
 - Tunnel mode..... 265
 - VPN Routes..... 270
 - VPN status..... 270
- IPSec VPN
 - configuring 271
 - configuring a Policy..... 278
 - defining remote keys.... 285
 - generate a client/host
certificate..... 292
- L2TP over IPSec
 - L2TP over IPSec client
parameters..... 289
 - L2TP over IPSec IP pool 289
 - L2TP over IPSec settings
..... 288
- Licensed Users 53
- Licensing 50
- Licensing Information 53
- Load Balancing
 - deleting rules..... 164
 - editing rules 164
- Load Balancing 163
- Load Balancing
 - defining rules..... 163
- Local Logs
 - Browse 312
 - configuring local log file
level 308
 - configuring remote log file
archive 309
 - filtering 315
 - filters..... 315
 - introduction 307
 - local log file archive 308
 - Local Log File Query 311
 - Log Files..... 316
 - remote log file archive.. 309
 - settings..... 307
 - starting search 311
- Local User
 - deleting..... 117
 - editing 117
- Local User
 - adding 115
- Log files
 - error codes 320
- Log Files
 - Admin notifications 318
 - Astaro Configuration
Manager..... 316

- Astaro User Authentication 316
- BIND name server 318
- Boot messages..... 316
- Configuration daemon .. 316
- Content Filter..... 316
- DHCP client 316
- DHCP server 316
- Fallback archive 316
- High Availability 317
- HTTP daemon 317
- HTTP proxy..... 318
- Intrusion Protection 317
- IPSec VPN 317
- Kernel..... 317
- Local Login 317
- Logging..... 317
- MiddleWare..... 317
- Network accounting
 - daemon 317
- Packet Filter..... 318
- POP3 proxy..... 318
- Portscan Detection..... 318
- PPPoE DSL dial-up 318
- PPTP VPN Access 318
- Selfmonitor..... 319
- SMTP proxy 319
- SOCKS proxy 319
- SSH remote login 319
- System log messages... 319
- Up2Date Service messages
 - 320
- Uplink Failover messages
 - 320
- Virus Protection..... 317
- WebAdmin access..... 317
- WebAdmin usage..... 320
- Log FTP Data Connections . 206
- Log Unique DNS Requests . 206
- Masquerading
 - deleting rules..... 162
 - editing rules 162
- Masquerading
 - defining rules..... 162
- Microsoft Outlook
 - creating rules..... 252
- MS Explorer
 - disabling proxy use 211
- NAT
 - defining rules..... 159
 - deleting rules..... 161
 - editing rules 161
 - introduction 157
- Network
 - adding 105
 - deleting..... 109
 - editing 109
 - filtering 108
 - introduction 103
- Network group
 - defining..... 106
- Networks
 - filters..... 108
- Networks 103
- Notification 118
- Packet Filter
 - advanced 203
 - system information 207
- Packet Filter Live Log..... 207
- Packet filter rule
 - adding/editing groups .. 194
 - enable, disable..... 194
 - sorting rules table..... 194
- Packet filter rules
 - rules table 193
- Packet Filter Rules
 - deleting..... 194
 - editing 194
 - filtering 195
 - filters..... 195
 - introduction 188
 - re-ordering 194
- Packet Filter Rules
 - setting 190
- Pattern Up2Date

Index

- installation, automatic 60
- installation, manual 60
- Ping
 - Using 178
- Ping Check..... 177
- POP3
 - configuring 232
 - Content Filter 233
 - header 235
 - Spam Protection 233
 - Virus Protection..... 233
- PPTP VPN
 - introduction 169
 - MS Windows 2000 Scenario
..... 171
 - PPTP Client Parameters 171
 - PPTP IP-pool 170
 - PPTP VPN access 169
- Protocols
 - AH..... 110, 112
 - ESP 110, 112
 - IP..... 112
 - TCP 110
 - UDP..... 110
- Proxy
 - DNS 227
 - HTTP 210
 - Ident 237
 - introduction 209
 - POP3 232
 - Proxy Content Manager 255
 - SMTP 238
 - SOCKS..... 229
- Proxy Content Manager
 - Age 256
 - deferred 256
 - filtering 258
 - filters..... 258
 - global actions..... 258
 - Mail-ID..... 255
 - permanent error..... 256
 - quarantined 256
 - Recipient(s) 257
 - Sender..... 256
 - smtp_queue 256
- Proxy disable
 - Netscape..... 210
- Quality of Service (QoS) ... 196
- Reporting
 - accounting..... 303
 - administration..... 298
 - Content Filter..... 301
 - current report 303
 - daily executive report by e-mail..... 302
 - DNS 302
 - executive report 302
 - hardware..... 299
 - HTTP proxy usage..... 302
 - Intrusion Protection 302
 - network 300
 - Packet Filter..... 301
 - PPTP/IPSec VPN 302
 - system information 305
 - virus..... 299
- Reporting
 - Accounting
 - configuring 304
- Restart 102
- Routing
 - introduction 155
 - kernel routing table 156
- Search
 - starting a search 333
- Search 333
- Secure Shell..... 48, 49
- Service
 - adding 111
 - deleting..... 114
 - editing 114
 - filtering 113
 - introduction 110
- Service group
 - defining..... 112
- Services
 - filters..... 113

- Services 110
- Settings.....44
- Shut down 102
- Shut down/Restart 102
- SMTP
 - block RCPT hacks 243
 - configure 239
 - DoS protection 239
 - encryption/authentication 241
 - Expression Filter 247
 - File Extension Filter..... 245
 - global whitelist 242
 - introduction 238
 - MIME Error Checking.... 244
 - postmaster address 239
 - Realtime Blackhole Lists 248
 - Sender Address Verification 248
 - Sender Blacklist..... 243
 - Spam Protection ... 248, 249
 - Virus Protection 246
 - Virus Protection/Content Filter 243
- SMTP Relay
 - Virus Protection 246
- SNMP Access
 - authorizing access 69
- SOCKS Proxy
 - configuring 230
- SOCKS Proxy
 - user authentication 230
- Static Routing
 - defining routes 156
 - introduction 155
- Strict TCP Session Handling 205
- Surf Protection
 - assigning profiles..... 225
 - categories 219
 - content removal 220
 - editing Surf Protection categories 216
 - enabling, profiles adding 221
 - introduction 215
 - profile assignment table 223
 - profile functions ... 218, 224
 - profiles editing 221
 - profiles table..... 217
 - URL blacklist 219
 - URL whitelist..... 218
- SYN Rate Limiter 204
- System Requirements
 - administration PC 20
 - example configuration 20
 - hardware..... 19
- System Time
 - automatic synchronization 47
 - manual configuration 46
- System Up2Date
 - installing 58
 - installing with HA solution 58
 - loading and installation, manual 56
 - loading, automatic 56
 - loading, local 57
- Time Settings 45
- Up2Date Service
 - introduction 54
 - Pattern Up2Date 59
 - System Up2Date 55
- Use external indicators 44
- User
 - filtering 116
- User Authentication
 - configuring LDAP 87
 - configuring MS Active Directory server 80
 - configuring Novell eDirectory Server 85
 - introduction 71
 - LDAP advanced 89
 - LDAP Server 78

Index

Microsoft IAS RADIUS		
configuration	73	
RADIUS.....	72	
SAM	76	
SAM – NT/2000/XP		
configuration	76	
User Authentication		
configuring OpenLDAP-		
Server	86	
Users		
filters.....	116	
introduction	114	
Users	114	
Validate Packet-Length	206	
WebAdmin		
blocking protection for		
Loggin attempts	93	
drop-down menus.....	38	
HTTPS.....	91	
info box	35	
kick	43	
lists	39	
menus	36	
online help	40	
refresh	41	
selection fields	36	
starting	43	
status light	36	
tab list	35	
WebAdmin Site Certificate...	94	

